Designing Secure Prisoner Computer Systems

Edition 1.25

Ron Fabre & Con Zymaris

Mar 25, 2018

ISBN 978-1-326-76383-1

Contents

Chapter 1

Preface

Audience

Familiarity with the operational demands of a high security correctional facility will be a valuable foundation, especially where this familiarity relates to inmate-facing technology.

The primary intended audience is prison management, engineers responsible for the design of a correctional facility, security consultants, and relevant policy and decision makers.

How To Contact Us

Please direct comments and questions concerning this publication to:

Ron Fabre <ron@cyber.com.au>
Con Zymaris <conz@cyber.com.au>

Chapter 2

Introduction

Advances in technology have brought an enormous range of benefits and efficiencies to all areas of society, and correctional institutions have been early adopters of many of these advances. From real-time RFID location tracking to biometrics, heart-beat sensors, iris scanners, microwave detectors, and more, prisons are not averse to implementing secure technological solutions. However correctional facilities have traditionally avoided inmate-facing computers due to the many security and safety concerns.

The deployment of computers in a correctional facility is a complex issue and mistakes can have serious consequences. Assuming these concerns can be solved, the introduction of computers into a correctional environment can bring substantial benefits to the prison, the inmates, and consequently to society as a whole.

This publication has been prepared to provide a prescriptive overview based on the authors' collective experiences in the field of Prisoner Interactive Learning System (PILS) solutions and in-cell interactive technology in prisons, allowing the reader to re-formulate the ideas and recipes provided for their jurisdiction and prison reality.

Inmate access to computers is inevitable and when done correctly the benefits outweigh the effort. By understanding not only the specifics of each risk outlined here, but also the thought-processes and rationale behind the mitigation, engineers who are planning for the deployment of computers for inmates can efficiently and economically address the relevant security issues.

One of the primary purposes of incarceration is to reduce the cost of offenders to society. This is achieved by incapacitation (to protect society) and rehabilitation[1], (so inmates become contributing societal members upon release). Computers are an inescapable part of the developed world, and computer education is therefore a critical part of an inmate's rehabilitation.

Inmate-facing computers can decrease prison operational costs. For example:

- Inmates are less likely to be bored and consequently enact the kinds of behaviours which are costly and destructive.
- Staff can remotely grant and revoke inmate privileges thereby reducing management overhead and risk to staff safety.
- Staff can enact automatic curfews on functions which would otherwise be unmanaged.
- Educational programmes and mental health counselling can be delivered remotely, reducing the costs otherwise associated with bringing external teaching staff and contractors into the prison.
- Computers can supplant numerous other entertainment devices, reducing the labour-intensive task of searching for physical contraband.

Computers can be valuable tools for inmate education in basic numeracy and literature and in further studies, both of which are required by modern society. Computers in prisons can also be used as vehicles for the delivery of focussed vocational training in many different disciplines.

Besides being used as conduits for training in a myriad of industries, knowledge of computers themselves is a benefit to all potential job-seekers. While professional office workers often spend their entire work day at a computer, tasks undertaken by non-professional workers also mandate computer skills as computers become increasingly ubiquitous. In order to maximise the chances that inmates will fit within modern society upon release, they too need contemporary computer skills.

Regardless of whether computers are used as a platform for general education or are there to give inmates direct computer skills, both assist in decreasing recidivism. This in turn can amount to a substantial saving for taxpayers.

[1] Retributive, incapacitative & deterrent theories of punishment are not discussed here.

Beyond the functional and financial advantages offered by computers in prisons there are also genuinely important human rights issues which need to be considered.

Correctional institutions in modern western societies provide their inmates with access to much the same fundamental privileges enjoyed by the general populace including medical care, exercise, entertainment, housing, heating, clean water, education, etc. Similarly, inmates should also have access to some of the services and information available on the Internet albeit limited, securely, and cost-effectively. Such access to the Internet is increasingly considered a fundamental human right[2].

[2] http://news.bbc.co.uk/2/hi/technology/8548190.stm

Chapter 3

Business Drivers

The fundamental purpose behind introducing computers into prisons is to assist with the rehabilitation of inmates and therefore reduce recidivism. This in-turn will reduce the cost to society of incarceration and of further criminal behaviour.

Some of the key facilitators for rehabilitation provided by computers in prisons are:

- Managed reintegration.
- Communicating with legal representation.
- Interaction with mental health and support resources during incarceration and continuing into the post release phase.
- Education - in-house and distance education/correspondence courses.
- Job seeking prior to release.

Inmates need computers because:

- Internet access is increasingly seen as a fundamental human right.
- Job seekers need computer skills as a core capability.
- Universities and other distance education providers increasingly require students to have computers.
- They offer entertainment through television, music, and games.

Correctional facilities need computers because they offer:

- Centralisation of education and entertainment requirements into one device.
- Improved management and curfew capabilities.
- Improved inmate disposition through reduced boredom and increased learning/rehabilitation opportunities.

The financial and societal costs of recidivism are high and consequently reducing those costs should be an effort of high priority. Making computers available as part of an overall programme of rehabilitation and reintegration should be part of that overall effort.

3.1 The Inevitability of Computers in Prisons

Due to the widespread availability of access to the internet, many educational institutions are making their distance learning content available solely via the Internet and expect students to communicate with instructors via email. Inmates without this access are at a distinct disadvantage compared to their non-incarcerated counterparts.

Most prisons in western countries today have programmes aimed at rehabilitating inmates by providing them with a valuable education in preparation for community reintegration. Access to suitable educational material is becoming easier and cheaper through computer-based resources, such as on-line distance learning courses offered by universities.

3.2 Costs of Re-offending

There are tremendous costs imposed on society and taxpayers due to inmates re-offending after release. This recidivism costs nations billions, and impacts countless lives; those associated with the victim and those with the

perpetrator.

In 'Making Prisons Work: Skills for Rehabilitation' (*[Justice11]*), the UK Ministry of Justice stated:

> "Re-offending blights lives and communities, carrying personal, social and economic costs of between £9.5 billion and £13 billion a year. Enabling offenders to have the skills that will make them attractive to employers so that they can find and keep jobs on release or whilst serving a community sentence - becoming an asset rather than a burden to society - makes sense. Whilst our investment in giving offenders the skills they need to help them get and keep jobs is significant, it is a fraction of the prize on offer to all of us if we can prevent the creation of future victims of crime, with the associated economic and social costs, by cutting their re-offending."

Because of these costs, strenuous efforts must be made to reduce re-offence and subsequent re-incarceration. Secure computers, available in prison cells, can play a substantial supporting role in this effort.

3.3 Work Driven Rehabilitation

In some jurisdictions, the focus on breaking the cycle of imprisonment puts work for offenders at the centre of rehabilitation. To prepare inmates for employment upon release, inmates must be given a work focus that instils decision-making, accountability and independence during incarceration.

In 'Making Prisons Work: Skills for Rehabilitation' (*[Justice11]*), the UK Ministry of Justice stated:

> "The roll-out of the virtual campus across prisons will be completed as quickly as possible within the constraints of a secure IT environment. This is essential in order to provide a modern skills environment and to make the important link to real jobs available outside. We will merge the prison careers information and advice service into the National Careers Service 2 to join up advice given in and outside custody. We will reshape careers advice in custody towards job planning for a successful job outcome post release, whilst continuing to identify those with a basic skills need early in their sentence so that we can address it. We will extend the use of intensive literacy and numeracy provision as a means of having an immediate impact in addressing functional skills needs of those with shorter sentences, but with a long term benefit that lasts well beyond the end of their time in custody. This will include addressing the issue that inmates are not always allocated to skills programmes despite having a clear learning need, and that people with learning difficulties and disabilities are not always assessed to allow their needs to be met. In doing this we understand that skills issues may not be the most immediate priority for some offenders - for example those with significant substance abuse or mental health issues - and that activity to address skills needs should take place once those more immediate issues have been resolved."

3.4 Virtual Hearings

It is a fairly common requirement in many correctional facilities for inmates to attend court. This is especially true for inmates on remand as the inmates' legal proceedings have not yet concluded.

The logistics of transporting an inmate securely out of a prison, to the court-house, and back in again afterwards are time-consuming. Correctional facilities that rely on RFID anklets and bracelets for location tracking face added complexities as these devices often must be removed from the inmate when they leave the facility, in case the inmate is released from custody by the court, and reattached if they do return.

To avoid these problems some correctional facilities are investigating and implementing videoconferencing[3] systems to enable inmates to participate in legal hearings without leaving the facility. The resulting financial benefits can be substantial.

In "'Virtual Hearings' Via Webcam Save Courts Money" (*[Huff11]*), Colleen Long reported:

> "The tools are used in courts large and small, and the savings for some are staggering: $30 million in Pennsylvania so far, $600,000 in Georgia, and $50,000 per year in transportation costs in Ohio."

[3] http://en.wikipedia.org/wiki/Videoconferencing

3.5 Education

Computers are no longer considered a luxury used in only a limited number of industries and work environments. Today, almost all job situations demand some interaction with a computer. Inmates therefore need an appropriate level of computer familiarisation and skills to help them improve their chances in the world beyond the correctional facility. Unless we prepare inmates to be able to retain such a job, we are relegating them to an extremely narrow job market opportunity such as manual labouring or similar.

To reduce recidivism, ex-offenders must have marketable job skills. Providing offenders with good work-place skills will make them more attractive to employers and thereby increase their chances of obtaining and maintaining employment post-release. While basic numeracy and literacy skills lay the foundation for academic and vocational training, computer skills are necessary in almost all employment scenarios.

In 'The Learning Prison' (*[OBrien10]*), Rachel O'Brien stated:

> "Nonetheless, we conclude that a bolder, 'ahead of the curve' case must be made for upgrading and modernising technology-enabled learning across the prison estate. Computers and electronic white boards are not treats for inmates but sensible ways to make return to the community more manageable."

3.5.1 Distance Learning

Education is one of the cornerstone activities which is used to rehabilitate inmates and help re-integrate those who have been released back into society. However there are often difficulties in getting educators or trainers to teach within prisons. This may be for any of the following reasons:

- Some prisons are a considerable distance from major population centres, making access to skilled educators difficult.
- Some subject-matter educators are rare, even within metropolitan centres.
- The logistics of getting educators into and out of a prison is a risky and time-costly exercise. They can be carriers of contraband, raising security risks by their presence.

Prison operators can do much to improve the process of inmate education by providing inmates with suitably locked-down and limited Internet access to approved educational institutions.

A policy permitting remote inmate access to educational resources offers prison operators a wider selection of competitive education providers beyond the local region.

3.5.2 Technology

The use of technology in general education and vocational training needs little evangelism. Computers and computer-delivered courseware are mainstays across most educational disciplines. Because educational institutions are moving towards online-only distribution, correctional institutions must cater for this eventuality.

In 'Making Prisons Work: Skills for Rehabilitation' (*[Justice11]*), the UK Ministry of Justice stated:

> "Having spent three years evaluating the VC, I am of the opinion that for offender-learners to gain maximum benefits from ETE opportunities, and for ETE provision to have the widest possible reach within prisons, the use of technology to deliver learning is an essential part of the offender learning strategy."

3.6 Reduction in Boredom

Many prisons today provide multimedia facilities to inmates, commonly in the form of televisions, radios, stereos, games consoles, and similar devices. They are valuable resources for reducing boredom, rewarding good behaviour by extending entertainment privileges, facilitating inmate education and rehabilitation, and for broadcast communication from staff to inmates.

When deployed securely, computers in cells can provide for the totality of inmate in-cell education and entertainment requirements.

3.7 Job Seeking

Increasing an inmate's chances of securing viable employment post-release is a major step towards successful re-integration.

In 'Promoting integration : the provision of prisoner post-release services' (*[Borzycki03]*), the authors stated:

> "The community can be protected in the longer term by minimising the likelihood of ex-inmates re-offending after they are released. One strategy for reducing the risk of recidivism is the provision of treatment, services and support to inmates during their incarceration and after their release. This paper examines various issues linked to the provision of post-release services to inmates, drawing on both international literature and a roundtable discussion held at the Australian Institute of Criminology in October 2002. Issues discussed include: obstacles to recently released inmates achieving community integration; facilitating inmates' return to mainstream society through provision of throughcare and post release services; promising trends in inmate rehabilitation; and throughcare practice and research needs in Australia. The paper also describes a model of throughcare delivery formulated by roundtable participants, which highlights the importance of interagency partnerships and the central role of floating care. This has its roots in the provision of accommodation, but can also be used in a broad range of services. In the case of post release interventions, floating care would involve a single case manager providing and/or brokering multi agency support to a client and his or her family, from a base in the offender's own home."

In 'REENTRY In Brief' (*[FIRC11]*), The US Council of State Governments Justice Center stated:

> "Reentry is an employment issue. Being employed is an important predictor of a former inmate's ability to stay crime free. While 2 out of every 3 men were employed before they were incarcerated, incarceration reduces their economic prospects substantially. A recent report from the Pew Charitable Trusts found that incarceration reduces annual employment by more than two months and reduces yearly earnings by 40 percent. Source: The Pew Charitable Trusts, 2010. Collateral Costs: Incarceration's Effect on Economic Mobility. Washington, DC."

To achieve this, access to job-search resources is critical. In many countries, online recruitment sites are the primary resource for job-seekers across all industries. To maximise chances of either gaining experience with the job market prospects or gaining employment, inmates who are due for release need to have access to the same resources.

In 'Australian Recruitment Practices' (*[Jepsen14]*), the authors stated:

> "Recruitment sourcing strategies have altered rapidly since 2000, with print media formerly the dominant form of recruitment advertising, to the internet being listed as the best source of information for Australian job seekers in the 2005 Going Global Career Guide. Carless (2007) noted that some 70 per cent of employers were using some form of online recruitment by 2005. "

3.8 Societal and Familial Reintegration

Managed reintegration strategies are necessary to strengthen and reunite families following incarceration, consequently decreasing the likelihood ex-offenders will re-offend, and can reduce the generational trend of ex-offender's children offending later in life.

Providing inmates with limited access to web and email resources enables correctional facilities to manage the progressive reintegration of inmates as they approach their release date.

Email interaction with partners, access to news and current affairs, and information about job prospects all offer powerful mechanisms to assist with the managed reintegration of inmates into society.

3.9 Preparation for Legal Proceedings

Inmates on remand need to be able to interact with their legal representatives, analyse evidence and prepare their defence. Often the legal teams are relying heavily on Evidence Management Systems for this purpose. A secure solution to enable remandees and their legal reps to communicate will reduce the number of physical visits, thereby reducing the associated security risks.

In 'Promoting integration : the provision of prisoner post-release services' (*[Borzycki03]*), the authors stated:

> 1.17 Remand inmates and all inmates who have legal matters pending, whether they are on remand or sentenced to a term of imprisonment, should:
>
> (i) be able to meet and have telephone conversations with their lawyers, consistent with security requirements; and
>
> (ii) have access to legal library resources, including where practicable supervised access to electronic media for the purpose of viewing electronic legal documentation.

3.10 Human Rights

Over 63% of the population in Europe use the Internet and it has consequently been recognised in law as a fundamental right on a par with freedom of expression[4]. Australia's uptake is considerably higher at almost 90%.

Inmates are generally afforded many of the basic rights that all citizens enjoy including clean water, health care, shelter, etc.

In general, the core human rights which are of particular relevance for inmates are the right to be treated with humanity, respect and dignity while incarcerated.

In 'Prisoners and Human Rights' (*[AHRC12]*), The Australian Human Rights Commission stated:

> "The United Nations Human Rights Committee has made it clear that prisoners enjoy all the rights in the International Covenant on Civil and Political Rights (ICCPR), subject to 'restrictions that are unavoidable in a closed environment'. (General Comment No.21)"

In jurisdictions permitting inmates political franchise, or the active right to vote, the inmates should have similar access to the sources of news and current affairs the general populace has. This in turn encourages a socially responsible outlook post-release.

In 'The right to vote is not enjoyed equally by all Australians' (*[AHRC10]*), The Australian Human Rights Commission stated:

> "... the Australian Human Rights Commission believes that enfranchisement is a powerful and positive tool to assist with social reintegration and rehabilitation of prisoners. Giving prisoners the right to vote would be consistent with Australia's obligation to ensure that: The penitentiary system shall comprise treatment of inmates the essential aim of which shall be their reformation and social rehabilitation."

Inmates of minority religions, who may otherwise be subjected to intolerance or bullying, can benefit from the opportunity to worship in the privacy of their cell. Video or audio recordings of religious services provided by any suitable place of worship (church, mosque, synagogue, etc) can be made available to the inmates to view privately.

3.11 Improved Management of In-cell Appliances

Inmates are often kept within their cells for many hours at a time. There is a need to keep them from getting bored, as boredom often introduces troublesome behaviour. For this reason technology devices within prison cells are common in many correctional facilities. Various jurisdictions allow inmates to have games consoles, DVD and CD players, computers, along with their TV sets.

[4] http://www.zdnet.com/eu-lawmakers-vote-to-introduce-net-neutrality-3039648565/

While there is broad agreement that it is to everyone's benefit that these technology devices are present in cells, there are also risks that are introduced. Any devices not specifically designed for use in prisons are a safety and security risk. Further, the more such devices that are allowed in cells, the greater the scope for problems.

Examples of the kinds of devices presently in prison cells which can be replaced by a secure computer are:

- Radio,
- CD player,
- Generic computer,
- DVD player,
- Television set,
- Digital set-top box,
- Games console.

Many benefits can be introduced by replacing these disparate inmate-facing appliances with a single manageable computer device. Rather than maintaining multiple devices per inmate, correctional facilities should incorporate all of these functions into a single secure and centrally managed device.

3.12 Delivery of Personal and Psychological Services

Therapy is an important aspect of an inmate's rehabilitative process. One of the more common forms is Cognitive Behavioural Therapy (CBT), which is seen as affecting long-term behavioural changes in offenders' behaviour.

Cognitive Behavioural Therapy (CBT) can be efficiently and effectively delivered online[5], making it particularly appropriate in a prison context.

Online delivery of CBT offers therapists and inmates greater flexibility in therapy session times and durations, allowing therapy to be dealt with promptly and privately. The correctional facility benefits from the reduced risk profile of therapists entering and exiting the facility, as they must do for face-to-face sessions.

Implemented securely, computers in cells are a valuable tool for delivery of therapeutic inmate services.

3.13 Improved Monitoring of Inmate Communications

Prisons generally allow inmates to correspond with a limited number of external parties by physical mail and telephone. Both of these activities are allowed in a strictly controlled and monitored manner, providing the prison with the level of surety the privileges are not being abused.

By introducing computers into cells, prisons have the option of selectively allowing inmates to send and receive email and to use Voice over IP (VoIP) telephony.

The key advantages of encouraging inmates to use these forms of communication are that they greatly enhance the monitoring capabilities available to prison staff while reducing their workloads. Through the judicious application of key-word and key-phrase filters and related software technologies, prisons can quickly capture more instances of policy-contravening email communication automatically, without requiring corrections staff to read each message as is necessary with physical mail.

Further, by appropriating existing policies such as the acceptable telephone usage policy, prison management can re-use existing frameworks of risk analysis and mitigation and inmates can quickly adjust to the email usage rules as they mirror the telephone usage rules.

[5] http://en.wikipedia.org/wiki/Cognitive_behavioral_therapy#Computerized_or_Internet-Delivered

Chapter 4

Design Considerations

When considering computer resources for inmate use within a correctional facility it is critical to first consider the entire design and resolve the serious security implications and risks. Many jurisdictions have attempted to introduce computers and have failed due to lack of planning or internal experience, attracting negative media attention and consequently causing the relevant authorities to remove the resources permanently.

As useful as computers are they have the potential to introduce new problems and it's prudent to address these *before* they become headline news.

Inmates must not be able to communicate clandestinely or hide any physical or digital contraband from prison staff. It is common for shared computing facilities to be at risk of infection by malicious software which, in a prison, can consequently threaten inmates' privacy and be an unnecessary administrative burden for staff.

The cost of the solution, both up-front and ongoing, should be considered. If cost-recovery measures are required then various methods of tracking resource utilisation must be evaluated.

As security is of paramount importance in the design and implementation of inmate-facing computing systems, multiple independent levels of security and a default-deny security policy must be employed throughout. In the event that a security mechanism is breached then multiple lines of defence must protect the system from further attack by hostile users, minimising the risk of inmates exploiting the system and ensuring staff have adequate warning of issues.

Consideration must first be given to a range of specific design and implementation issues, and care must be taken to avoid commercial-off-the-shelf (COTS) solutions as neither corporate nor home computing systems are viable or safe for prisons. Taking a naive COTS approach *will* attract problems, however all of these problems are avoided by following the techniques in this document as has been demonstrated for many years by successful implementations in other jurisdictions.

4.1 Unproven Software in Prisons

Commercial desktop software is generally designed to allow the user to do most anything they care to do, as convenience is easier to sell than security.

Most desktop application software assumes the user is either a benign or friendly entity, whereas in prisons the inmate users must be treated as potentially hostile entities. Furthermore, the inmates have a great deal of time on their hands and high levels of motivation to attempt to escalate privileges and access resources or capabilities that are forbidden to them.

The risk profile within a prison setting exceeds that of a home or commercial environment, so the systems and services provided to inmates must adhere to a higher standard and must be built from the ground up to not trust the users.

Deploying any kind of inmate-facing computer solution which doesn't have a multi-year operational presence in prisons is taking serious unnecessary risks. When embarking on such a project it is important to consider similar projects implemented at other prisons and learn from their successes and failures.

4.2 Retro-fitting Existing Facilities

Incorporating the necessary communications infrastructure into an existing and populated correctional facility can be a complex and perhaps expensive venture.

It is important to locate the core servers and communications equipment where inmates are forbidden, ensuring the inmates are provided no opportunity to access the system management console and hardware.

Due consideration must be given to surface-mount cabling conduits in areas frequented by inmates. Exposed steel conduit can be used as an anchor point for rope and cable can be tied as a noose, which is a risk for inmate self-harm. Plastic conduit, however, may offer opportunities for hiding physical contraband. Where possible, cabling should be embedded within the building walls.

Where there is no existing network cabling within an established facility there may be existing cabling (eg; analogue coax/TV, intercom/phone line) which will be made superfluous by the new networked solution. If there is no remaining 'draw-wire' in the subterranean conduits and pits then the old cable can be used to draw the new network cable through.

Chapter 5

Risk Mitigation

Before diving into the specific risks and strategies for mitigation, some terms of art must be introduced:

Defense in depth Security is arranged such that an attacker must defeat multiple heterogeneous layers of security[6] to achieve a malicious objective. For example, protecting a window with both metal bars and a motion sensor.

Principle of least privilege Resources are only made available when they're needed for legitimate use[7]. For example, chef's knives might be available to inmates preparing food in the kitchen, but not at other times or locations, and never by other inmates.

AAA Protocol (Authentication, Authorisation, and Accounting)[8]

Authentication, within the context of computer systems, is the act of confirming the validity of the claimed identity of the user. This is commonly achieved by comparing the user's password against the central authentication database.

Authorisation is the level of access to resources which a user, or group of users, is permitted once their identity has been verified. This permission can then be granted or revoked by staff.

Accounting is the tracking and logging of access to resources by users as part of an audit trail.

Jail-break Removing the software restrictions on a device imposed by the vendor, usually with the intent to install supplemental third-party software.

COTS (Commercial off-the-Shelf) Refers to consumer grade appliances or services available from common vendors and retailers. For computers this typically means computers designed for corporate or domestic environments.

BIOS (Basic Input/Output System) The interface between the computer hardware and the operating system. The configuration of the BIOS is typically accessed during the early stage of the computer booting.

Live CD A full operating system booting from removable media, usually CD or USB key.

Privilege Escalation A user obtaining privileges they are not explicitly authorised to have. These privileges are usually gained when a system has a bug that allows security to be bypassed or, alternatively, has flawed design assumptions about how it will be used.

Malware (Malicious Software)

Any software used to disrupt or damage the computer system, gather sensitive information, or gain unauthorised access. Common forms of malware includes viruses[9], keyloggers[10], spyware[11], trojans[12], and backdoors[13].

Each issue below will first describe a "user story" - how the attack could be carried out - then describe techniques to mitigate the attack. To make examples more tangible, named individuals are used:

Charlie inmate, child sex offender.

Terry inmate, technically competent.

[6] https://en.wikipedia.org/wiki/Multiple_Independent_Levels_of_Security
[7] https://en.wikipedia.org/wiki/Security_engineering#Security_stance ("default deny")
[8] https://en.wikipedia.org/wiki/AAA_protocol
[9] https://en.wikipedia.org/wiki/Computer_virus
[10] https://en.wikipedia.org/wiki/Keystroke_logging
[11] https://en.wikipedia.org/wiki/Spyware
[12] https://en.wikipedia.org/wiki/Trojan_horse_(computing)
[13] https://en.wikipedia.org/wiki/Backdoor_(computing)

Jack, James inmate, assault charges & badly-behaved.

William inmate, well-behaved victim.

Thomas inmate, trans-gendered.

Anaru inmate, Bahá'í (religious minority) worshipper.

Ethan inmate, embezzler.

Steve inmate, organized crime soldier.

Oliver organized crime boss, not an inmate.

Warren prosecution witness, not an inmate.

Ben staff, bent/malicious.

Daniel staff, dim-witted.

Ian staff, intel officer.

5.1 Improvised Weapons and Self-Harm

A careful analysis must be made of all equipment prior to introduction in a prison setting, especially where the inmates are considered violent or are at risk of self-harm. *COTS* computer hardware with full-size keyboards, full-length cables, and full-size desktop or tower cases are unsafe and insecure for use in a prison environment. For example, flail weapons can be fashioned from power bricks, keyboards and mice.

User Story

James has a laptop computer which he is using for his studies. He takes the heavy power adapter and, holding the hard-wired cable, uses the adapter as a cosh or flail weapon against William.

Fig. 5.1: External Power Adapter

User Story

At the end of class, Jack surreptitiously removes a keyboard cable and makes an improvised garrotte which he then uses against Charlie.

User Story

While in his cell Steve breaks an optical disc (CD or DVD), creating a sharp-edged blade, and uses it to harm himself.

All computers must have internal power supplies, and all peripherals should be light-weight or non-removable where possible.

All computer cables (keyboard, mouse, power, and network) should be limited to 300mm/12" in length. This requires the room layout, specifically in regards the placement of wall-points, take short cabling into account.

As a short mouse cable may make the mouse unnecessarily difficult to use when connected directly to the computer, suitable sockets should be incorporated into the keyboard so the mouse can be 'daisy chained' off it. A socket at each end of the keyboard will offer convenience for both right-handed and left-handed users.

The content of all optical discs should be cached in a controlled environment allowing staff to provide inmates with access to the content but not to the physical media. This is best solved by storing the content of the media on a centrally managed server where access can be controlled on a suitably limited basis.

5.2 Concealment of Physical Contraband

The chassis of COTS electrical appliances have many obscure cavities inside which physical contraband (written note, shim pick, razor blade, illicit drugs) can be trivially hidden.

A spot-check of such devices for physical contraband can take substantial time, often half-an-hour or more depending on the complexity of the chassis and peripherals. If the policy of the prison is to check each appliance at least once per month (which is arguably too broad a time-frame) then it could be a full-time job for one person to manage a small quantity of devices.

User Story

Terry softens the end of a toothbrush with a cigarette lighter, pushes it into a screw head in the back of his computer, then lets it set again. With this he is able to gain enough torque to open the chassis and hide a shim pick under the lid of the computer.

User Story

Jack and James have a history of causing trouble and hence are not permitted to fraternise. Jack opens the battery compartment of the wireless keyboard or mouse in the library and hides a written note for later collection by James. Jack and James continue to use this method to clandestinely communicate.

User Story

James has a television, a CD player, a radio, and a game console in his cell. In the cavity of one of these appliances he hides a small mobile phone (smuggled in by Ben) which goes undetected for some months. Due to the substantial number of appliances, and the lack of time available, Daniel fails to find the contraband during a routine spot-check.

Toiletries and similar items must not be thermoplastic material (cf. thermosetting), to prevent their use as makeshift moulded tools.

The *All-in-One* computer chassis profile offers less cavities than a common desktop computer. Additionally this profile occupies less desk space and requires fewer external cables (e.g. video and audio).

Deployment of a *transparent computer chassis*, usually made of strong acrylic, can help by exposing hidden cavities and simplifying and speeding up spot-checks. The staff's ability to inspect the equipment more quickly and efficiently can decrease the ability of inmates predicting a routine. Note, however, that acrylic chassis may not include adequate electro-magnetic shielding[14] as required by some jurisdictions.

Regardless of which chassis profile is selected, the hardware manufacturer must secure the chassis with Tamper-Resistant Torx (often referred to as 'Torx TR') or pin-in Torx screws to make removal difficult without the correct tool.

[14] https://en.wikipedia.org/wiki/Electromagnetic_compatibility

Fig. 5.2: Example All-in-One Computer Chassis

Fig. 5.3: Example Transparent Computer Chassis

Tamper-evident tape should be applied to show clear evidence of access to the chassis of the device, however this is more of a reactionary strategy and implies that staff will become aware of the infraction only after the fact. This shifts the attack to the tape; a discussion of attacks on tamper-evident tape is available in §14.4 of *[Anderson08]*.

Fig. 5.4: Tamper-Resistant Torx Screw Head

A single computer can provide television, video, multi-media, and gaming functionality, reducing the number of devices requiring regular inspection.

5.3 Digital Contraband

Digital or electronic contraband can take many forms, from simple typed notes to graphical or video child pornography.

The risk of digital contraband can be a complex issue to solve. Challenges include the increasingly large and often obfuscated file storage systems present in general-purpose computers, and the support for small removable file storage devices in COTS computers, portable media players, set-top-boxes, DVD players, portable tablets, and games consoles. If inmates are able to boot from non-approved media (i.e. USB or optical media) then other strategies listed here will have no effect.

This is also a serious issue that *must* be shown to be thoroughly addressed in any prison computer solution due to the often politically damaging nature of uncontrolled contraband being discovered within a prison.

User Story

Charlie is permitted to watch DVDs on a computer in his cell. He looks through them for a brief adult nudity scene. He takes a screenshot of the genitalia and uses an image editor to superimpose them on the image of a (clothed) child. He now has ersatz child pornography.

User Story

Ben brings in a USB key with copies of a few popular movies for Jack's consumption on a computer in the prison. Jack then uses this as a tradeable commodity with other inmates.

Any screenshot functionality should be disabled, and computers should not make image editing software available to inmates who are likely to abuse the privilege.

Computers must have no uncontrolled common storage that inmates can take advantage of. Inmates must not be able to read any storage writeable by other inmates. Desktops should have no local storage at all, in case inmates exploit the system and gain elevated privileges.

Computers must prevent inmate access to writeable mass storage, such as USB thumb drives and optical media. The system must allow access to only those USB devices explicitly whitelisted, and foreign devices must be rejected and staff alerted to their presence.

Any email solution must restrict unapproved attachments, including images.

5.4 Unidentified Printed Documents

The printing of hardcopy documents is a commonplace requirement with any full-functioning computer system, particularly one used for working through educational courseware, however printers can also be used to create hardcopies of contraband material, such as inappropriate imagery. It is therefore imperative that the originator of any printed material can be easily identified.

User Story

James obtains some images containing pornography and, from his cell, prints it to the library printer. The librarian retrieves the hardcopy before James is able to, however neither the librarian nor Ian (the intel officer) are able to identify James as the culprit.

All printed documents must include information on every page, in a watermark or header, explicitly identifying the inmate who printed the document and the date and time the document was printed. Electronic copies of all printouts must be retained and stored securely in a non-modifiable format (e.g. PDF) for staff to review at a later time if required.

This is effectively impossible to achieve in a secure manner on a per-application basis and therefore should instead be implemented within the underlying printing subsystem.

5.5 Clandestine Communication

The nature of a computer system as a communication tool implies the presence of a myriad of potential risks for clandestine communication, and therefore implementation of a computer solution first requires careful design and consideration of all risks to mitigate against each of these risks.

Examples of mechanisms by which inmates may clandestinely communicate are:

- Shared document storage areas used as a virtual dead drop for electronic documents.

- Email systems which allow non-text content to pass through without quarantine, thus enabling hidden communications within attachments.
- Embedded WiFi devices facilitating isolated peer-to-peer networks.
- Unified inmate and staff networks, reducing the protection against inmates utilising a staff account on the system and taking advantage of the elevated privileges gained.
- Lack of secure firewalls on any computer devices (including desktops and servers) which would otherwise ensure isolation from each other.
- Misconfigured switch infrastructure, allowing end-points to communicate with each other directly.
- Inmates logging in with the same account on physically separate desktops and sharing documents stored in the home directory.

User Story

Jack and James have a history of causing trouble and hence are not permitted to fraternise. On a local hard-drive of a computer in the library Jack hides a document containing a typed message for later collection by James. Jack and James continue to use this method to clandestinely communicate.

User Story

Oliver sends Steve an email with a photo of a text document attached. The attachment includes instructions to kill Ethan. The facility's email system keyword filter fails to identify the email as hostile because it is unable to recognise and process the text in the graphic image.

There must be no shared document storage areas to which inmates have write access. Inmates must be able to store and edit documents in only their personal home directory where no other inmates have access and staff can review the contents from the central management console without warning.

The central management console should allow staff to define blacklists of keywords and key-phrases for flagging, and per-inmate lists of approved addressees with which the inmate is permitted to correspond. The facility's policy for inmate telephone use can be applied to email services.

The email solution must automatically analyse all correspondence in real-time, scanning for pre-defined keywords, attachments, and unapproved sender-recipient combinations. Messages which fail any filter should be quarantined for staff review, however neither the sender nor the recipient need be aware of the review.

During introduction of any computer device staff must be check it to ensure there are no wireless communications devices contained within, and that inmates are unable to later install and utilise any similar device they may acquire (see also *Wireless Communication Devices*).

The underlying network infrastructure must isolate the inmate, staff and management networks from each other, and must isolate all end-user nodes from each other (see also *Rogue Devices*). This increases the protection against inmates attempting to make use of staff credentials, of inmates probing and attacking other services (e.g. the Integrated Library System), and foreign devices successfully communicating directly with each other.

The system must prevent inmates from logging into more than one device at a time (see also *Concurrent Logins*), or to subsequently login to a system service with a different user account.

5.6 Clandestine Monitoring

It is important for prison staff to be able to clandestinely monitor all inmate behaviour in real-time and, where practicable, to review the history of their behaviour. For example, inmates are typically watched on CCTV camera, while the history of relevant activities would be viewed through archival videos.

Any inmate computer system should provide staff with similar oversight and an efficient mechanism by which they can 'see' or monitor what any specific inmate is doing at that time in a manner which is undetectable by the inmate under observation.

Besides allowing prison staff to gain evidence for actual policy abuses, the knowledge among inmates that they could be under constant observation will in turn ameliorate their behaviour.

User Story

From their behaviour, Ian suspects Jack and James are communicating, but the method eludes him. He can see they're using the computer, but the surveillance cameras lack the resolution to see detail on their screens.

Inmates must understand they are offered these privileges on the condition their behaviour may be under direct observation and often without their immediate awareness. When the inmate logs into the desktop the system should display the 'acceptable use policy' and request the inmate explicitly accept the policy before allowing them to use the resources.

At a minimum, the management console must include a remote control application which offers a 'monitor only' mode whereby the inmate is not alerted of the staff member's virtual presence and the console's keystrokes and mouse movements are suppressed.

All system activity must be logged, and these logs stored securely away from inmate access (see also *Log Retention*). The logs must be available to staff in a format that is easy to review and export, allowing staff to isolate the information they need by focusing on a subset of the log entries pertaining to only a specific inmate, desktop, date, and/or service.

5.7 Rogue Media

Any storage device which is portable and outside of staff control can be considered rogue media including CDs, DVDs, USB keys, SD, CF cards, and legacy floppy disks.

An inmate can store any manner of digital information on such media which can then be passed around within the prison, perhaps smuggled out of the prison, or otherwise used in a manner outside of the control of the prison staff.

Fig. 5.5: Example media storage devices

When looking at the risks that rogue media entails, three kinds of information must be separately considered - data, programs, and complete operating systems.

User Story

At home, Ben downloads a pornographic video onto several writable DVDs. He smuggles the DVD media into the facility and sells them to various inmates, who use them for personal entertainment and as a valuable trade-able commodity.

User Story

Charlie gets a "mix tape" music CD from a friend. It has a hidden data track that contains child pornography, which is ignored by stereos, but which he can access through a computer.

User Story

Oliver researches inmate and staff personal information, loads it onto a common micro SD card (15×11×1mm, ¼g), and uses a bow and arrow to fire it over the perimeter wall and into the exercise yard. It is easily concealed and passed to Steve, Oliver's soldier inside the prison. Steve reads it on the library computer and uses the information to blackmail other inmates and staff.

User Story

Ben has deployed a number of computers in the education room for use by inmates attending regular classes. Ben did remove unapproved and inappropriate software from the computers, however Terry finds that the operating system recovery partition allows him to reinstall these components.

User Story

After six months, a number of computers have broken down. Charlie is computer-literate and so Daniel puts him in charge of repairing the broken computers. Charlie tells Daniel that his testing requires a *live CD*, and tells him where to download it from. Because Charlie can now boot directly from the CD, he can evade network monitoring and study the network to find vulnerabilities.

The desktops must allow access to only approved optical media, and deny access to any discs not previously reviewed and approved by staff. Upon detection of unapproved optical media the system must alert staff of the attempt.

Typical optical discs consist of multiple music tracks, a single track containing movie content, or a single track containing documents or applications. It is rare for an optical disc to contain a mix of different track types, and in a correctional facility the presence of such media may be an attempt to hide electronic contraband.

The desktops must analyse any optical media upon insertion and if an unusual data structure is detected then access to the disc must be denied and staff alerted.

Computers must be configured to deny use of any removable storage devices, other than perhaps optical media, and to actively alert staff of such attempts. Support for these devices must be removed from the operating system kernel and users must be denied the ability to activate kernel modules or drivers.

COTS desktop computers are often supplied with a recovery partition to allow the user to repair simple software faults or install new drivers as required. This is not acceptable in a correctional setting, so removal of any such partition is mandatory.

Computers must be configured to prevent booting from any removable media including optical discs (see also *Booting From Insecure Media*).

5.8 Rogue Devices

There is a large variety of devices which may be introduced into a vulnerable network which can serve to both weaken the prison computing system's security as well as reduce system management effectiveness.

Unapproved computer devices on the inmate network introduce risks of contraband storage, unattended system vulnerability analysis, traffic sniffing, and so on.

An unmanaged computer introduced onto the network, such as an educator's laptop, can be a major vector for risky functionality or software.

Embedded computer devices are becoming increasingly ubiquitous and appearing in such appliances as media players, DVD players, refrigerators, *set-top boxes* and modern digital TV sets. Many of these devices can be trivially exploited to create rogue computing platforms for illicit use by inmates.

Fig. 5.6: Example digital set-top box (image retrieved from Wikipedia, 2014-09-05)

Many hobbyist suppliers and electronic component stores have small *full-function computer devices* available for retail purchase, such as the SheevaPlug[15] or Intel Edison[16].

Fig. 5.7: Example SheevaPlug embedded computer

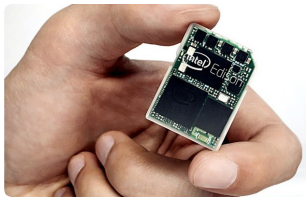

Fig. 5.8: Example Intel Edison computer

User Story

The local free-to-air televisions stations are due to begin the cut-over from analogue to digital transmission. To ensure continued television services the prison staff deploy COTS digital set-top-boxes in the cells.

Unknown to staff, the set-top-boxes are small computers with full support for USB, internal storage and network access, and file-sharing capabilities.

Terry discovers the capabilities of the set-top-box in his cell, connects it to the nearest data point, and then creates a bootable disc for other inmates to boot their networked computers to access the set-top-box as a rudimentary server. Inmates are able to store and share digital contraband of all sorts and evade detection.

[15] https://en.wikipedia.org/wiki/SheevaPlug
[16] http://www.intel.com/content/www/us/en/do-it-yourself/edison.html

User Story

Terry convinces Daniel to smuggle in a SheevaPlug, a small computer that closely resembles a common power adaptor. Terry is then able to use this computer for any malicious means such as network attacks or storage of digital contraband.

User Story

As a reward for good behaviour, William is permitted an Xbox game console in his cell. He is strong-armed by Jack who then coerces Terry into *jail-breaking* the console so that it can run arbitrary networked applications.

User Story

Steve has a mobile phone smuggled into the facility. He keeps the mobile phone charged by connecting it to the digital TV or set-top box in his cell, and evades detection because the TVs and set-top boxes send no alerts to staff.

The network switches must support 'port isolation', or private VLANing[17], to prevent communication between client devices. All devices must be permitted to communicate with only approved server(s).

Each network wall-point must be restricted to allow only a specific approved MAC address[18], and to alert staff and be disabled upon detection of a foreign MAC address on that port.

Unmanaged digital televisions and set-top boxes should not be used in a correctional facility. Video content can instead be provided to inmates through a managed multi-purpose computer platform which is configured to actively alert staff of misuse or upon detection of contraband.

Desktops should be configured to immediately power-down if network connectivity is lost or if the network connection is unavailable when booting up. This reduces the opportunity for inmates to evade detection when connecting contraband devices.

Any mains-powered devices which include USB ports must not offer more than the minimal required amperage on those ports. Computer USB ports generally offer up to 2.0 amperes, however a keyboard and mouse requires no more than 0.1 amperes. Limiting the output power accordingly will reduce inmates' ability to use low-powered devices (eg; hand-made tattoo guns, mobile phones, etc).

5.9 Denial of Service Attacks

A denial of service attack makes an approved system or service unavailable to the legitimate user or users. Denial of service attacks are common on public networks, such as the Internet, but are also a viable attack mechanism with any shared computing resource or network.

An example from the physical world would be a vandal damaging a public telephone, thereby denying others the legitimate use of it.

User Story

Jack is in a computer class, but wants to go and smoke in the yard instead. He creates a document on the server, and keeps creating copies until no space remains. Because nobody can save files the class is cancelled, enabling him to go out to the yard.

[17] https://en.wikipedia.org/wiki/Private_VLAN
[18] https://en.wikipedia.org/wiki/MAC_address

User Story

While using one of the computers in the library, James prints a substantial number of documents, expecting the supply of paper in the printer to be exhausted. The librarian leaves the room to get more paper, and James has a few minutes unsupervised to bully Anaru.

User Story

Since phone calls are expensive but emails cost him nothing, Ethan starts "sexting" his girlfriend by email from his cell at night. This results in hundreds of short emails for Ian to check the next morning. Because of the volume of messages requiring review, Ian starts skipping some, including coded orders from Oliver to his soldier Steve.

System storage quotas must be implemented so that individual users are unable to fill the entire file-system. They may be able to fill their own quota however this will impact only themselves and not the rest of the class or the prison population.

Printing services should be available to desktops in only the immediate vicinity of the printer. Service curfews should be implemented to ensure printing is permitted only while staff are in attendance.

Logging of printing, including who printed the document and when it was printed, must be in place so that such abuse can be tracked back to the specific inmate (see also *Unidentified printed documents*).

Email resource throttling should be implemented, delaying delivery of individual messages for a pre-defined period (e.g. fifteen minutes). Further, a daily or per-recipient hard-limit should be set to reduce the total amount of email an inmate can send or receive.

5.10 Uncontrolled Data Storage

Broadly, there are three forms of persistent data storage mechanisms:

- local, removable media (e.g. DVD, CD, USB key, SD card)
- local, internal media (e.g. hard-drives)
- remote, network storage (e.g. file server)

Most COTS computers come delivered with an internal hard-drive containing the operating system, assorted applications, and capacity for personal data storage.

For maximum security, a prison computing solution must be designed to exclude and prohibit all forms of data storage that cannot be completely managed, locked-down, and inspected without warning. Only networked, server-based storage should be used. The internal hard drives in personal computers must be removed, and removable media blocked completely.

User Story

Unknown to other inmates, William is collaborating with the police investigator in a court case involving Oliver. William has been preparing a document on his computer for the investigator which includes evidence of Oliver's criminal activities. Oliver is suspicious of William's involvement with the police and consequently instructs Steve to investigate.

While William is away from his cell visiting with his lawyer, Steve goes into William's cell to access his computer. Steve finds the document and confirms William's intentions. He deletes the document and later kills William in the gym, thereby destroying the evidence central to the case.

User Story

Using the word-processor on the library computer, Steve writes a document asking Oliver to silence Warren (a witness for the prosecution, giving evidence against Steve). Steve posts the letter to his wife who then passes it on to Oliver.

All data must be stored in a controlled environment on the central server. Each inmate must have their own personal file storage directory on the server which is securely isolated from all other inmates. Only the relevant inmate and delegated prison staff can be permitted to gain access to each inmate's data. This ensures other inmates cannot gain unauthorised access to these documents.

Inmate computers must not include any local persistent storage (hard-drives or removable writeable media) as this pushes enforcement down to the inmate environment where it does not belong.

Automated document scanning tools must be implemented to scan the contents of documents and alert staff of relevant contextual phrases or keywords. Staff can then review such documents and take action as required.

5.11 Malicious Software

All of the external threats that apply to a corporate or domestic IT environment also apply to a prison computer environment.

User Story

Thomas is permitted to use an educational CD which includes an application pertinent to one of the classes he is taking. Unknown to him, the application installs a computer virus which later activates and deletes system files and all of Thomas' home-work.

The computer system must restrict applications from gaining *elevated privileges* and prevent inmates from installing or running unapproved software.

Each desktop should revert to the approved SOE[19] upon reboot, and enforce regular reboots, thereby providing an extra layer of protection against errant software.

5.12 Log Retention

It is critical that all system activity is recorded automatically in logs, however the logging and retention policy usually provided with COTS computer systems is insufficient to meet the demands of a correctional environment.

In "Information Security Manual Controls" (*[ISM14]*), the Australian Department of Defense stated:

> "Since event logs can assist in reviews, audits and investigations, logs should ideally be retained for the life of the system and potentially longer. The retention requirement for these records under National Archives of Australia's (NAA's) Administrative Functions Disposal Authority is a minimum of 7 years after action is completed."

User Story

During a routine inspection a pornographic DVD is discovered in Jack's cell. Ian consequently reviews the system logs and identifies the DVD has been changing hands for at least the last two months however he is unable to ascertain the circumstances of the original appearance of the media because the logs expire after two months.

[19] https://en.wikipedia.org/wiki/Standard_Operating_Environment

Activity must be recorded for every relevant interaction that both inmates and staff have with the computer system. The logs must be centrally located in a highly-secured area of the system, and not on any computers or network resources accessible by inmates. Staff must be able to manage, sort, search and filter the logs through a variety of open-ended tools so that the information sought by prison technical staff can be discovered.

The system logging mechanism must retain all log entries for a number of years. A reasonable guide to apply to the system logs is the same retention policy applied to the site-wide security camera video footage.

The types of activity which must be recorded includes:

- Attempts to login to the desktops and to individual services
- Powering on and off an inmate computer
- Insertion of CDs/DVDs
- Attempted use of contraband devices (WiFi, USB, etc.)
- Launching of applications, both approved and prohibited
- Email metadata (who sent it, when, to whom, etc.)
- Email content and attachments
- Accessing internal or external network resources (Intranet, file-server, Internet)

The logs should be used not only for post-issue analysis but also pro-actively. The system should automatically alert staff upon detection of certain activities, allowing staff to take prompt action and avoid further occurrences.

5.13 Permissive Software

Most software applications are written for corporate or home audiences and without consideration for the strict requirements of a correctional environment. As such, many applications include unwelcome functionality which is a security risk but which is not immediately obvious to the casual or untrained observer.

Unwelcome insecure functionality includes:

- A command prompt or terminal
- Encryption (of documents or data)
- Non-sandboxed scripting subsystem which interacts beyond the specific application (e.g. VBA scripting in Microsoft Excel)

User Story

Charlie discovers the CAD package on his computer includes a terminal window. This is incredibly useful for probing for vulnerabilities, because he can write arbitrary scripts and immediately see their results.

All software must be subjected to an in-depth assessment ensuring it doesn't provide features that inmates can abuse.

New versions of applications often introduce not only welcome bug-fixes but also unexpected new functionality, therefore this assessment must be revisited during every subsequent upgrade or refresh.

5.14 Webcams

Webcams are generally unwelcome in most prisons due to the risk of their use to communicate with other parties or to capture still images or videos.

In prisons where webcams are forbidden, or on those computers which do not require the devices, care must be taken when procuring computers to ensure they do not include embedded webcams. Additionally, the operating

system must not include drivers for webcams and the kernel must refuse attempts by the user to load kernel modules or hardware drivers.

5.15 Wireless Communication Devices

There are many small electronic *wireless communications devices* available which offer peer-to-peer or internet communication capabilities including mobile phones, 3G modems, WiFi dongles, and Bluetooth adapters. All of these can be serious risks to the security of a correctional facility, allowing inmates uncontrolled communication with each other and with external parties.

A locked-down WiFi implementation offers strong security, however there remains a higher risk that this one layer of security can be exploited or bypassed (see also *Defense in depth*).

Many prisons are introducing 3G suppression or jamming devices. These kinds of technical countermeasures are useful but not fool-proof, as due to the nature of the technologies involved, rapid change means that the technical countermeasures may be superseded and then bypassed.

Fig. 5.9: Example USB communications device

User Story

Oliver tapes a USB 3G adapter to a quadrotor UAV. He flies it over the perimeter fences and into the yard, where Steve collects it. Steve connects it to a computer, and has full internet access. This enables Steve to communicate in real-time with Oliver.

User Story

Charlie pays Ben to smuggle him an USB bluetooth reader. He connects it to a computer and instructs it to alert him to nearby devices. Charlie now knows when guards are near, because their cellphones automatically connect to the reader when in range.

Computers must be configured to deny installation and use of unauthorised applications or hardware devices, and to actively alert staff of such attempts. Support for these devices must be removed from the operating system kernel and the system must be deny users the ability to activate new kernel modules and hardware drivers.

5.16 Unauthenticated Access

Basic computer security dictates that access to resources must be granted only in combination with user authentication (see also *Authentication*), and this is no less important within a prison environment. By authenticating an inmate, it is possible to allocate requisite privileges, block specific resources, deliver customised policies or procedures and create an auditable trail of activity.

User Story

OPAC[20] (library catalog) kiosks are set up in the library, and can be used by inmates without logging in. In an act of simple vandalism, an inmate regularly replaces the desktop wall-paper with an inappropriate image. Staff do not have logs with identifying information enabling them to identify which inmate is doing this.

[20] https://en.wikipedia.org/wiki/Online_public_access_catalog

The computer system must deny unauthorised access to all resources and all activity must be logged correctly (see also *Log Retention*).

All system services should rely on a single authentication back-end database. This includes the desktop itself and any hosted services (e.g. Integrated Library System). This reduces the risk of exposure of a poor implementation within any one application and allows the system greater opportunity for central control and activity logging.

5.17 Concurrent Logins

A 'concurrent login' is where a single user account is used on multiple disparate devices or system services at the same time, whether by the same legitimate user or by multiple users sharing the same account.

User Story

Jack shares his login details with James. After lock-down, both login as "Jack" and create a document in Jack's home directory. James hits "refresh" on Jack's document and vice-versa, allowing both to communicate in real-time without detection because Ian reviews inmate files only during his day shift.

When an inmate successfully authenticates against any service the computer system must actively scan for existing login sessions and, where it finds a matching session, it must reject the new session and forcibly log the user out.

Any violations of this policy should trigger an exponential back-off[21] of the authentication service, effectively punishing the inmate by not allowing them to login again for a period of time, however not enacting staff intervention which would otherwise be required to re-enable the account. Further violations can lead only to extended periods of time where the inmate is unable to abuse the system.

5.18 Mismatched Authentication

Most general-purpose computers allow a user to login with one account and then to access secondary services (e.g. GMail or netbanking) with an unrelated account. This flexibility is acceptable in an office or home setting however it can lead to security issues in a prison context.

Inmates must not be able to login to the desktop with one user account and into a secondary service with a different user account.

User Story

Jack and James have learned through experience they can't login to separate computers as the same user, so instead they login to their respective computers as themselves and then both login to the email service as Jack.

Jack and James also know Ian regularly scans and reviews email in the inmate Inbox and Sent Items folders, so now they leave messages for each other in Jack's "Drafts" email folder (and never send them).

[21] https://en.wikipedia.org/wiki/Exponential_backoff

All services requiring authentication and which are accessible through the computer (e.g. Integrated Library Service, email, legal database) must confirm the user account matches the account authenticated on the desktop itself.

Due to the centralised nature of the services, the desktop will need to regularly (e.g. every 20 seconds) confirm with the server if the desktop user account matches the server-based services being accessed. Upon detection of a violation the session must be immediately terminated, the account locked, and staff alerted.

5.19 Shared Authentication

It is important to accurately identify the inmate utilising the computer desktop or service. If the inmate sitting at the computer does not match the account they're using then inappropriate privileges will likely be made available to the wrong inmate.

User Story

James' system account is locked by staff due to bad behaviour, so he stands over William until William tells James his password. Now James can log in as William and retain computer access.

The management console should provide staff the ability to restrict individual desktop computers to specific inmates or groups of inmates. For example, the computer in cottage three would be restricted to only the inhabitants of that cottage, ensuring none of those inmates can utilise account credentials obtained from other inmates.

If the correctional facility is relying on physical location tracking devices (e.g. RFID bracelets/anklets) or biometric devices (e.g. fingerprint or optical scanners) then the computer solution should make use of its location data to confirm the inmate is actually in the location of the desktop where the inmate's account is being used.

5.20 Desktop SOE Maintenance

Old and unmaintained software will often have long-running vulnerabilities which can be exploited by inmates. Such vulnerabilities may offer inmates elevated privileges or allow them to bypass security restrictions in the system.

Updating the software on even a single computer can take a non-trivial amount of time, especially where the computer has no access to any online software repositories provided by the vendor. Regular maintenance of the software on a large number of independent computers normally requires that technical staff perform the maintenance in-situ or that the computers are retrieved and serviced in a secure location before being returned to the inmate population. This is a labour-intensive burden on staff which is impractical and does not scale well beyond a small number of computers.

Software updates must be performed over the network from a secure central location, ensuring technical staff are not required to perform their duties in the inmate areas and minimising the continual relocation of computer systems.

Shared SOEs[22], stored on a server and distributed to the desktops on demand, will substantially reduce the software maintenance effort and enable staff to quickly revert to earlier versions of software if necessary.

5.21 Curfews

A policy of restricting inmate access to privileges or areas per the time of day is common practice within correctional facilities. Curfews limit access to locations and resources, and are a necessary part of the command and control structure in a secured facility.

[22] https://en.wikipedia.org/wiki/Standard_Operating_Environment

Problems can occur when introducing computer technology into a prison without first ensuring its ability to control included services per established curfew policies.

User Story

Ethan stays up long into the early hours of the morning watching TV. Next morning he falls asleep during class, is irritable and gets into a fight with Jack.

User Story

Charlie is using the library computer while the librarian is out on break getting lunch. While unsupervised, Charlie uses the opportunity to print pornographic images on the library printer.

All services must be subject to automated and pre-defined curfews. Examples of suitable curfews includes:

- TV services should be available on the cell desktops only during lock-down hours, and no later than mid-night.
- Printing services should be available only during the hours the librarian is expected to be in attendance, such as 2pm to 3pm.

Prior to a system curfew being enacted the desktop should give the logged-in user sufficient warning to allow them to save any documents they're currently working on.

5.22 Removal of Privileges

Prison staff need to have a mechanism by which relevant privileges can be revoked from inmates and in a manner which obviates potentially risky confrontations.

Isolated and unmanaged devices cannot easily be deactivated remotely, so staff are generally required to enter the cell to remove the device. With this in mind, general purpose or common-of-the-shelf computers are unsuitable in a correctional environment.

User Story

Daniel wants to punish Jack's bad behaviour by removing the Xbox and TV from his cell, but Jack is in there and feels like fighting. Daniel requires the assistance of three more staff members to provide protection and assistance, thereby taking them away from other duties.

The central management console for the inmate-facing computer system must provide staff with a high level of control of the inmate services and devices which is both flexible and granular, allowing staff to respond promptly and appropriately to policy violations, and from a position of safety.

Staff should be able to immediately restrict an individual service, such as television, games, or audio, from a specific inmate or a group of inmates. Conversely, reinstatement of privileges should be an equally simple task.

5.23 Unpatched Software

One of the most commonly exploited vulnerabilities in any computer system is through old unpatched software. Any non-trivial software system has bugs or vulnerabilities, and some of these allow users to perform prohibited actions or otherwise exploit that software, other software on the same system, or the underlying computer hardware or network.

User Story

The inmate kiosk in the library has been running for two years without security updates. Charlie remembers a vulnerability announced before he was incarcerated six months ago, and uses this to escalate privileges to the local administrative account on this computer.

The software vendor's security errata must be monitored on an ongoing basis to pro-actively identify potential vulnerabilities. Access to the security errata may require a suitable support agreement be reached with the software vendor.

All relevant patches for inmate-facing software must be applied promptly (see also *Permissive software*) after the vendor makes them available. In those instances where a patch is not yet available for a known vulnerability then the relevant software application should be immediately removed from the inmate desktops, pending later availability of a patch.

5.24 Booting from Insecure Media

There are serious security implications associated with insecure bootable media as such devices can contain full operating systems, prohibited software, and illicit documents. Booting a computer device (computer, tablet, set-top-box) into an unapproved operating system gives an inmate access to tools or pathways which would otherwise be entirely blocked, raising possibilities for clandestine communication, unfettered access to wireless communications technologies, and unmonitored contraband digital content such as pornography.

Almost all general-purpose personal computers such as desktop PCs, laptops and servers, can boot from removable media. Many other computers with non-traditional profiles, such as tablets and smart-phones, can also boot from removable media.

The *BIOS* shipped in typical COTS computers allows the user to selectively boot from removable media. While the BIOS can normally be protected against unauthorised changes with an administrative password, there are safeguards present which allow the user to bypass this protection and reconfigure the BIOS. These safeguards are usually a motherboard jumper, a removable battery, and the BIOS detecting multiple incomplete reboots in quick succession.

User Story

Charlie smuggles in a *live CD*. His computer's BIOS is configured to only boot from the network, and is protected with a password, but Charlie knows that by flicking the power switch on and off rapidly he can reset the BIOS configuration back to the manufacturer's factory default settings. He does so, and can boot the live CD. He now has full control over his computer, can reset the local administrator password, and can execute non-approved programs from the CD.

In most cases the BIOS shipped in COTS computers is unacceptable for use in a secure prison environment. When selecting hardware for inmate use it is critical that hardware be chosen whereby the BIOS denies inmates the ability to enact any illegitimate change and a factory default reset returns the system to a known-good and secure state. It is insufficient to rely on simple password protection of the BIOS, regardless of how tightly configured the BIOS is.

5.25 Concealment of Staff Identities

In some jurisdictions, prison policy dictates that the identity of staff and services contractors must be protected from the inmates. Any computer system deployed at a prison must adhere to this policy.

Inmates must not have access to the full names or personal contact information of correctional staff.

User Story

By listing the system home directory, Steve obtains the full names of staff from the computer system. Steve exfiltrates this information to Oliver, who looks them up in the phone-book and Facebook and sends accomplices to threaten staff family members.

The staff home directories must be isolated from the inmate home directories, perhaps on separate file-systems, and inmates must have no access to the former.

All staff accounts must be created without reference to their common name. A reasonable format for the username could match their staff number, and perhaps with a prefix 'S'. e.g. John Smith's staff number is 6782, so his login ID is s6782. Any evidence of his login ID would expose no useful identifying information.

Generic account names (e.g. intel, librarian, admin) must not be used as they make auditing and log analysis difficult. Each staff member must have exactly one account.

5.26 Software Developed In-house

The correctional facility, or the relevant government department responsible for the facility, is unlikely to have sufficient in-house skills to design, develop, and maintain a useful application secure enough for inmate use. In the rare instance where this is not the case, such staff are valuable and more likely to leave for the private sector, thereby leaving a technical skill void.

User Story

The prison relied on an internal technical staff member to develop an Integrated Library System[23] for the library, intended for use by inmates to catalogue the books and publications available to them.

Over time, the technical staff member moved on from the prison, leaving a gap in the technical expertise available at the prison. Previously undetected vulnerabilities are now being exploited by Terry to allow him to clandestinely communicate with other inmates.

[23] https://en.wikipedia.org/wiki/Integrated_library_system

It is important to first investigate existing COTS solutions designed specifically for inmate use. A commercial partner will bring experience obtained through projects from other correctional facilities and allow the prison to take advantage of features and functionality first tested elsewhere.

5.27 Public Kiosks

OPAC[24] kiosks usually lack a full keyboard and therefore require a touchscreen interface, however must also be resilient to vandalism. The touchscreen surface should be rated a minimum IK10 and the kiosk chassis a minimum IP66[25].

The touchscreen device should require no calibration (as with resistive technologies) however the common alternative of a capacitive interface does not meet vandal resistant standards. The solution is infra-red touchscreen devices which need no calibration tuning and can support the required IK10 rating.

If a printer is required within the kiosk chassis then one should be deployed which avoids jamming and demands a minimum of ongoing maintenance.

Laser printers often can be positioned so the paper slides out of the output tray when released from the printer. The inmate is therefore unable to yank the paper from the printer, damaging the unit or jamming the paper path. Laser printers do still jam on occasion and often need consumables (e.g. paper and toner) replaced.

[24] https://en.wikipedia.org/wiki/Online_public_access_catalog
[25] http://en.wikipedia.org/wiki/EN_62262

Heat-sensitive printers normally support a relatively large amount of paper on a spool and do not use toner therefore the consumables maintenance is minimal. Additionally, heat-sensitive printers are less prone to paper jams than laser printers are. Note though that the paper format in heat-sensitive printers is usually different to that of a laser printer, usually less than half the width of standard A4 or letter size paper.

5.28 Tablets and E-book Readers

In recent years, portable tablet devices and eBook readers have become common in commercial, educational, and home environments due in part to their convenience and portability. Some education providers consequently view these devices as potentially viable mechanisms for distribution of educational content to the inmates for these same reasons.

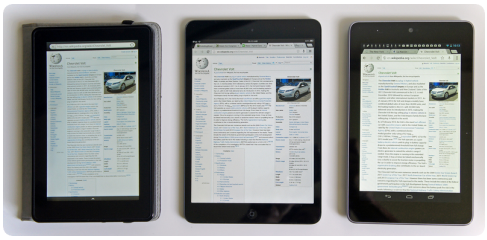

Fig. 5.10: Example Tablet Computers

Some of the more general risks associated with these portable devices have been covered elsewhere in this document (e.g. *Rogue Devices*, *Digital Contraband*, *Uncontrolled Data Storage*, *Log Retention*), however there are other issues and risks which are more specific to this device profile.

The battery life of a common tablet computer ranges from two hours to perhaps ten hours, depending on the battery quality and assuming ideal usage conditions. The implication is the inmate must have access to a power source to recharge the device, or they must regularly return the device to an authorised staff member to recharge it on their behalf. Many of these devices are recharged through a standard USB socket, so providing an inmate with access to a suitable USB power adaptor also enables the inmate to recharge other contraband devices (e.g. a mobile phone smuggled into the facility).

Removal of contraband devices (e.g. 3G, WiFi, Webcam) from a COTS tablet or e-book reader is generally not possible because all components are tightly integrated into a single circuit-board. Disabling of these devices through software can be difficult and there can be no surety the inmate won't re-enable the devices.

Chapter 6

Cost Recovery

The total expenditure of implementing and operating an inmate-facing computer system can be substantial, regardless of whether COTS or bespoke. A cost-benefit or cost-recovery analysis may be required before embarking on the project.

The cost of the solution needs to be justifiable or recoverable, depending on the policy of the jurisdiction. Different jurisdictions have varying policies with respect to the funding of inmate services. In some, the general policy is to charge-back the cost of services, while in other jurisdictions these costs might be invested by the prison.

6.1 Government or Facility Funded

Some of the issues to consider in determining the costs vs benefits are the cost of incarceration per inmate, the amortised cost of implementation and ongoing support of the system, and the number of inmates expected to be positively impacted by the solution and thereby not returning to prison.

A hypothetical facility with 500 beds and an annual cost per inmate of $100,000 is aiming for a reduction in recidivism of just 1%. The projected benefit in this case, over the 5 year operational lifespan or depreciation schedule of the project, would be $2.5 million.

6.2 Inmate Funded

Where the costs of services are borne by the inmates then the ongoing utilisation of these services must be accurately tracked and reported on. The solution may need to be flexible enough to allow staff to provide education resources at no cost to the inmates and yet recover the costs of entertainment activities.

6.2.1 Printer Resource Utilisation

There is a reasonable expectation that printing resources will incur a charge-back facility, such as when people pay the local office suppliers, copy-shop, or library for photocopied or printed material.

All printing activity should be logged, enabling corrections staff to track how much printing each individual inmate is doing and providing the correctional facility the ability to on-charge the specific inmate for their usage. The printer accounting facility ideally could cater for cost differentiation on whether the page is colour or monotone, and allow integration with any existing quota framework.

6.2.2 Rental Plans or System Utilisation

A rental plan can be implemented where a single unit is rented to an inmate for a set cost (e.g. $5 per week). This strategy can increase the perceived value of the device and thereby reduce the chances of misuse and vandalism, however is unlikely to be successful in environments where non-paying inmates can take advantage of the device.

Prison management might consider a post-paid strategy based on consumption of the service. The system should track how long the inmate is logged into the desktop and record this detail in a central database. Staff can then charge the inmate for their usage of the desktop.

A better strategy involves the inmates pre-paying for the service, and matches the common paradigm of a pre-paid mobile phone service. As with the post-paid strategy, the system should track how long the inmate is logged into the desktop, but should automatically and forcibly end the session when the inmate's account is depleted.

This should be integrated with the quota mechanism ensuring inmates can use the service for only a predefined amount of time per session thereby allowing a fair distribution of computer availability to all inmates. This may reduce motive for personal conflict between inmates.

6.2.3 Internet Traffic Consumption

Inmates may be charged on a per-email basis, in much the same way that stamps are purchased when posting physical letters. Similarly, their usage of web traffic can be metered and on-charged to them, in the same way that a home ISP will bill for data.

In both cases this should be implemented on the server, following the same cost-recovery strategy (post-paid vs pre-paid) as applied to the desktop itself and cutting off the service for that inmate if their account is depleted.

6.2.4 Television and Streaming Media

Viewing of television and streaming media services through the computer can allow staff to charge for usage on a per-channel (or per-stream) basis.

Prison management should be able to charge a premium for channels offering primarily entertainment content, however charge less for internal channels on containing educational or health content.

Bibliography

[Anderson08] Ross Anderson (2008). Security Engineering - A Guide to Building Dependable Distributed Systems. Wiley. ISBN 0-470-06852-3.

[Justice11] Ministry of Justice (2011). Making Prisons Work: Skills for Rehabilitation. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/230260/11-828-making-prisons-work-skills-for-rehabilitation.pdf

[OBrien10] Rachel O'Brien (2010). The Royal Society for the encouragement of Arts, Manufactures and Commerce. The Learning prison. http://www.thersa.org/__data/assets/pdf_file/0006/278925/RSA_The-Learning-Prison-report.pdf

[Borzycki03] Maria Borzycki and Eileen Baldry (2003). Promoting integration : the provision of prisoner post-release services. http://www.aic.gov.au/publications/current%20series/tandi/261-280/tandi262.html

[FIRC11] Federal Interagency Reentry Council (2011). REENTRY In Brief. http://csgjusticecenter.org/documents/0000/1059/Reentry_Brief.pdf

[Jepsen14] Denise Jepsen, et al. (2014). Macquarie University. Australian Recruitment Practices: A Literature Review on current Australian recruitment practices for Australian Workforce and Productivity Agency. http://www.awpa.gov.au/publications/Documents/Australian%20recruitment%20practices%20report.pdf

[AHRC12] Australian Human Rights Commission (2012). Prisoners and Human Rights. https://www.humanrights.gov.au/prisoners-rights

[AHRC10] Australian Human Rights Commission (2010). The right to vote is not enjoyed equally by all Australians. http://www.humanrights.gov.au/human_rights/vote/index.html

[Huff11] Colleen Long (2011). Huffington Post. 'Virtual Hearings' Via Webcam Save Courts Money. http://www.huffingtonpost.com/2011/05/09/virtual-hearing-webcam-court_n_859331.html

[ISM14] Australian Department of Defense (2014). Australian Government Information Security Manual Controls. http://www.asd.gov.au/publications/Information_Security_Manual_2014_Controls.pdf

Index