THE Open GROUP

Boundaryless Information Flow

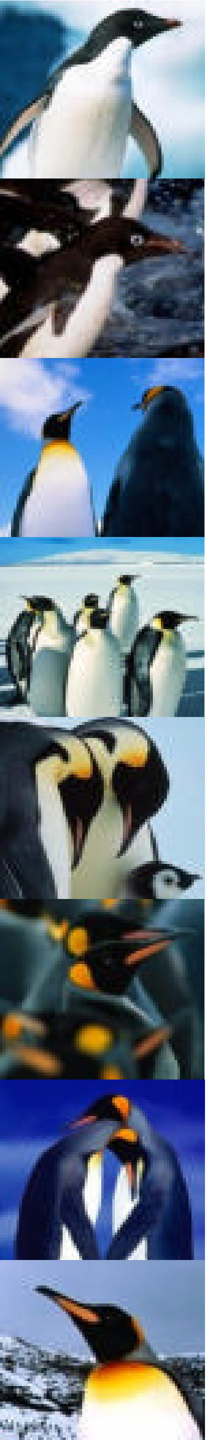
Boundaryless Information Flow

Open Source in the Enterprise

September 8, 2003
Hilton London Paddington
London, UK

The impact of Open Source on IT security

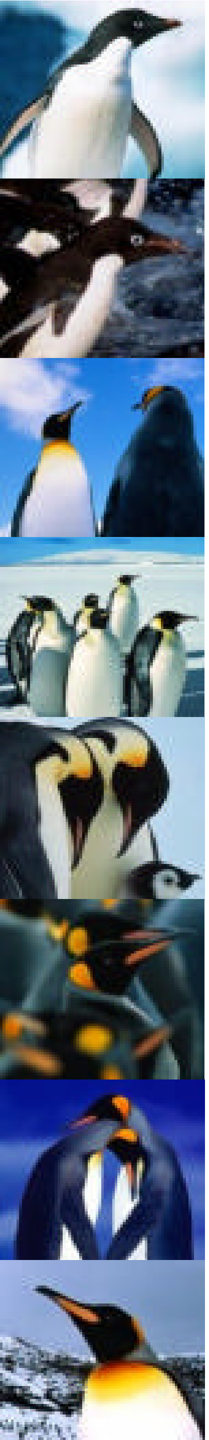
A source of joy or conflict?



What is our market?

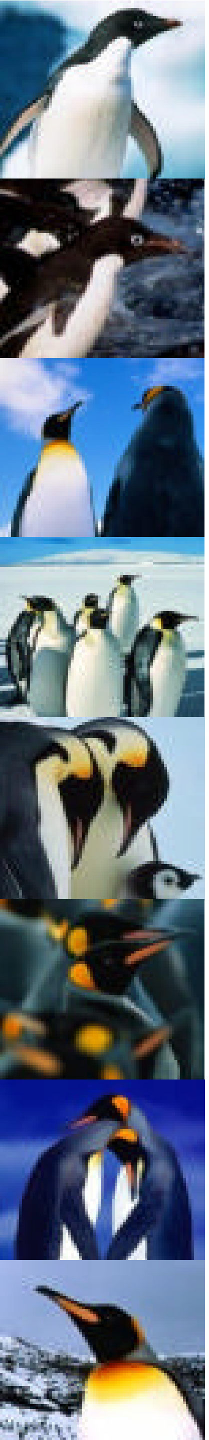
COMPUTER SECURITY

- We publish easy to install, easy to use products for file, folder, archive and content encryption
- We deliver customers visible ROI
- We work with all major PKI vendor keys and the OpenPGP standard
- We are e-mail and application neutral



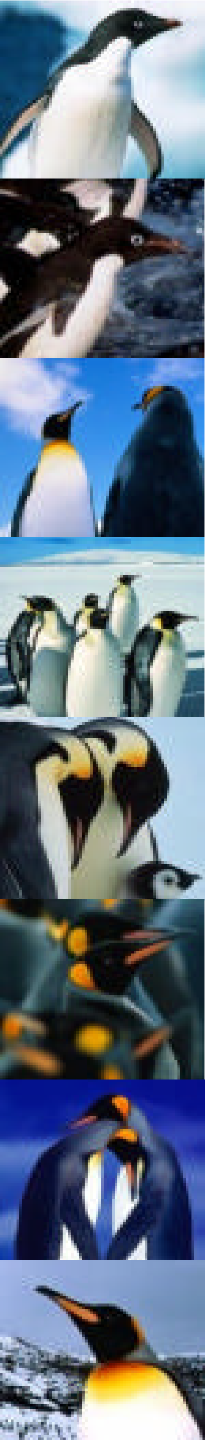
What pressures are we under?

- Quality
- Safety
- Reliability
- Dependability



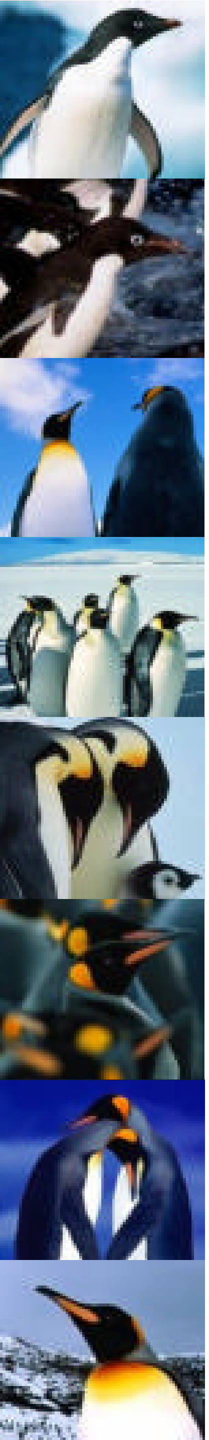
History of the security sector

- Marginal at best
- Industry leaders have failed to deliver
- Security claims too often damned by poor performance or through inept implementation
- Failure to engage the user
- Ruled by fashion and politics



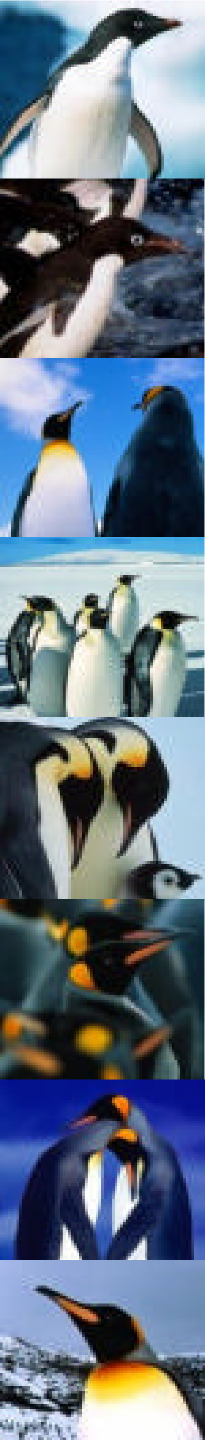
Security public requirements

- Need to be able to demonstrate provenance clearly to the (often) self-appointed assessors
- Need to remedy any failures very quickly indeed
- Need to defend against claims for negligence



Security private problems

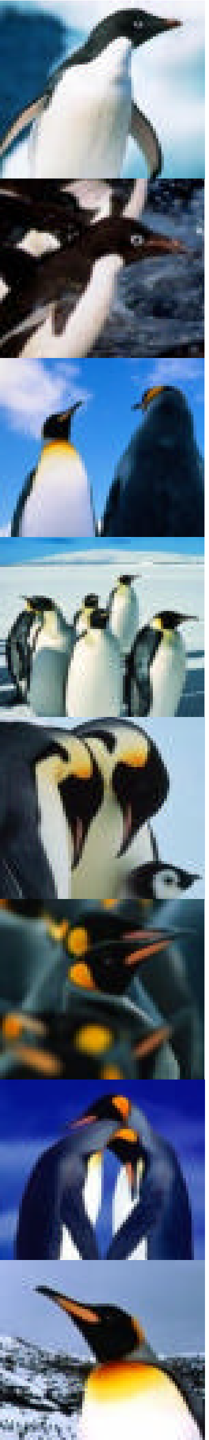
- How to protect intellectual capital
- How to delay the ability of competitors to interoperate with or supercede your capabilities
- How to ensure quality operation without exposure to internal error
- How to avoid being compromised
- How to sell what some think is free software



Catch-22

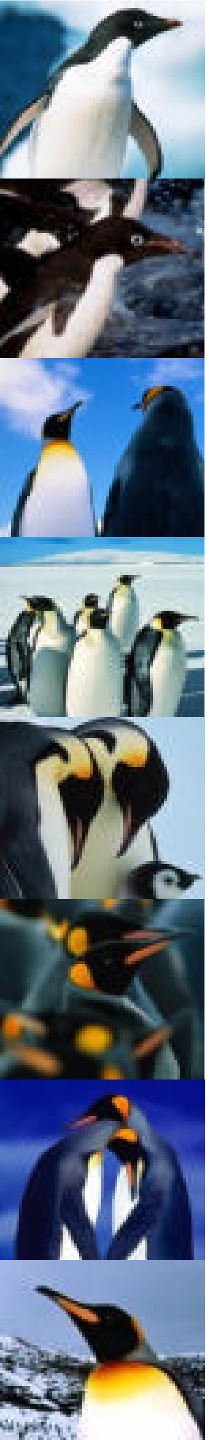
“There was only one catch and that was Catch-22, which specified that a concern for one's safety in the face of dangers that were real and immediate was the process of a rational mind.”

Joseph Heller



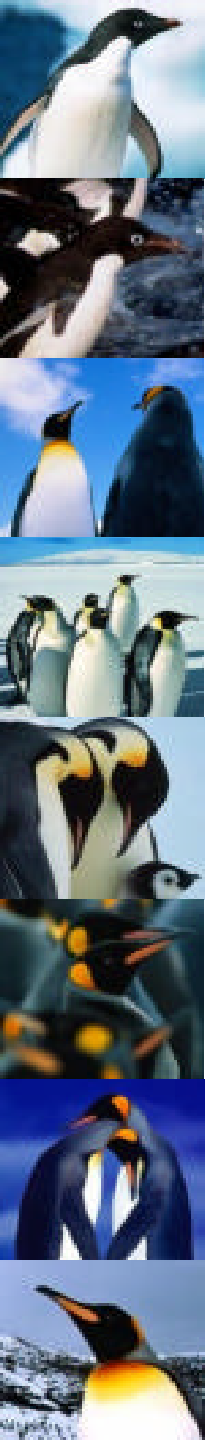
Catch-22

- To satisfy the public you must publish your entire source code BUT the ITSEC warn that the longer the attacker has access to the system the easier it will be for them to compromise the system



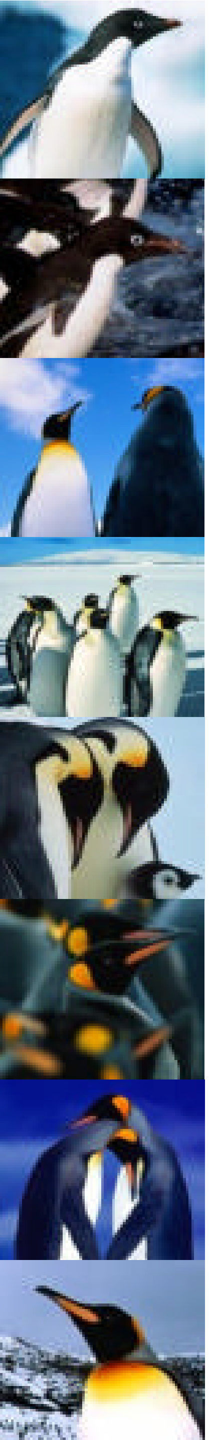
Catch-22

- Poor algorithm implementation is the commonest source of compromise BUT algorithm libraries are commonly subject to patent control, licensing or other controls



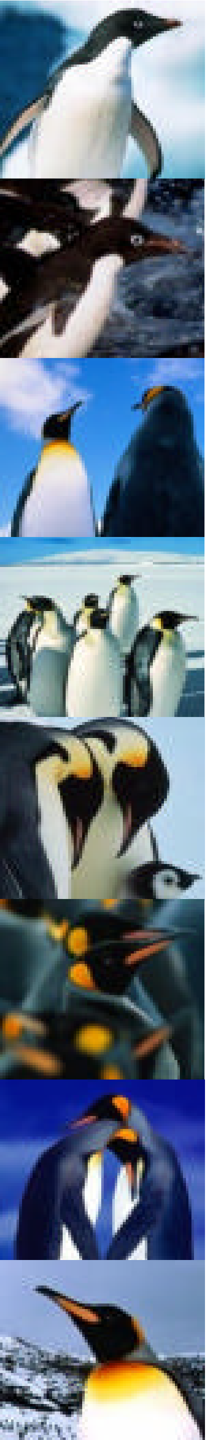
Approaches?

- Open Source
  - Superficially attractive – it means that you can properly claim that your source has been publicly inspected – or at least it is open to public inspection, even if no-one of any merit has actually studied it in detail
  - Problems – actually it’s licensed – what are the terms – what do you do if source you rely on is shown to be flawed but you can’t fix it – what terms must you obey – what compromise do you leave yourself open to? – what must you ‘give away’



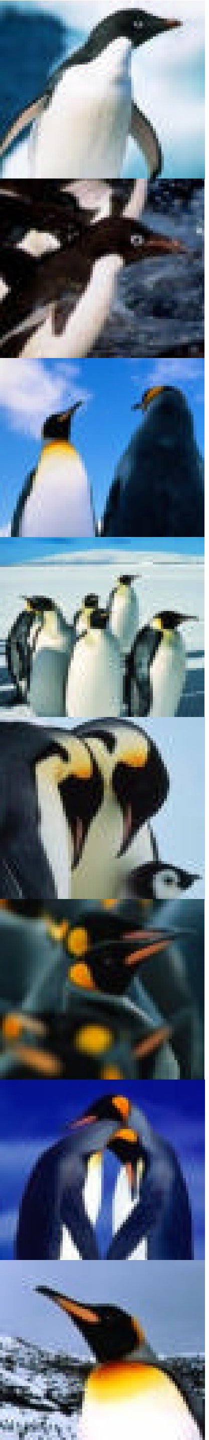
Approaches?

- Proprietary source
  - Superficially attractive – can have trade secrets – patents – makes it more difficult for the attackers to try and subvert the system – you can control your destiny
  - Problems – your ability to attack your own product(s) may be limited by resource or by expertise or by vision – you may not be aware of errors if you do not have to interoperate with ‘foreign’ systems – your users may not be able to test your products any more reliably than you can



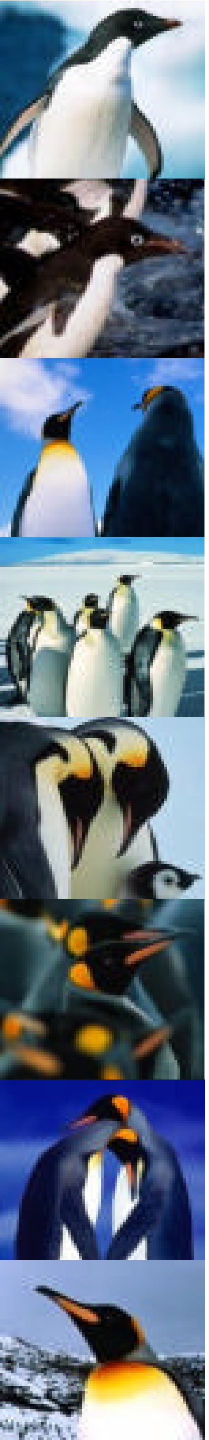
Approaches?

- Proprietary source with certification
  - Superficially attractive – it solves the problem(s) of disclosure and may obtain an expert overview and assistance – it allows corrections to be made out of the public gaze – national bodies available
  - Problems – cost may become an barrier to market entry for smaller organizations – a new layer of complexity – costs have to be passed on to customers so sales price may unreasonable – many evaluation schemes are suitable for military rather than domestic – can you trust your military? – what happens if it does fail?



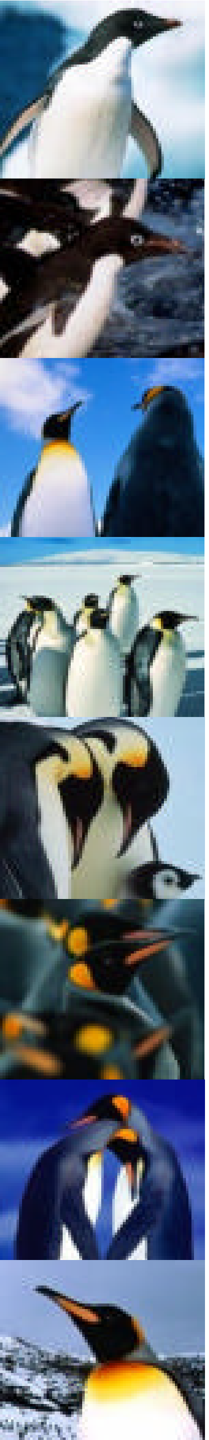
A third way?

- Well, perhaps not, if only because the phrase has political tarnish and arithmetically speaking it is option 4



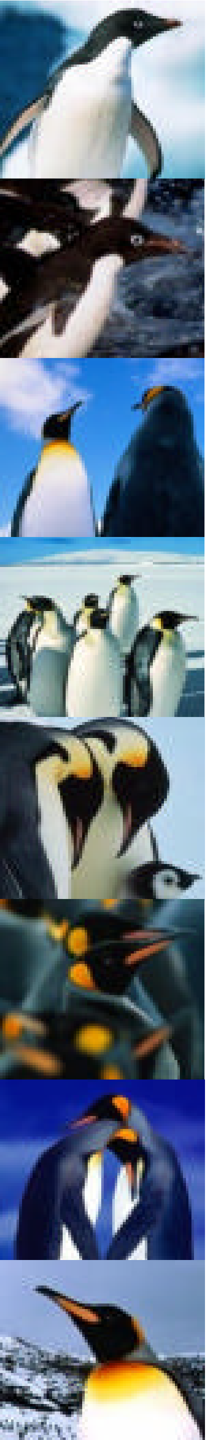
Compromise – what we did

- Use Open Source when it fulfils the customer’s requirements for disclosure and public review
- Use proprietary source when the customer need not be concerned over what is actually happening
- Use best practice (if you can find any) to ensure that you do not compromise the benefit of using the Open Source



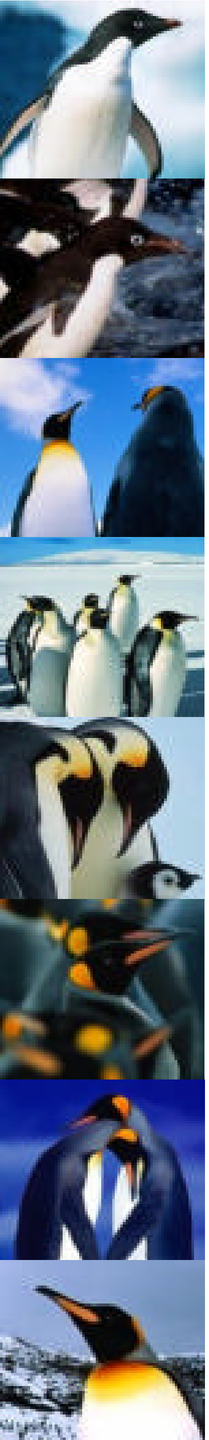
What specifically?

- Our encryption algorithms are all Open Source from the Legion of the Bouncy Castle, and random bitstreams are taken from Infinite Monkey
- Everything else is proprietary
- We interoperate with other providers, so that any faults in our own implementation would be revealed by their systems



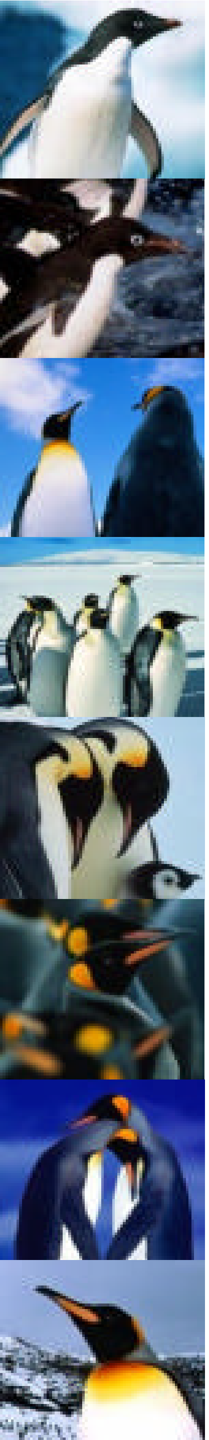
Does it work?

- For most customers, yes.
- They can check interoperation easily for themselves without having to be technically inclined.
- They can see the references for Open Source and satisfy themselves quickly that we are using those libraries and what their provenance is.



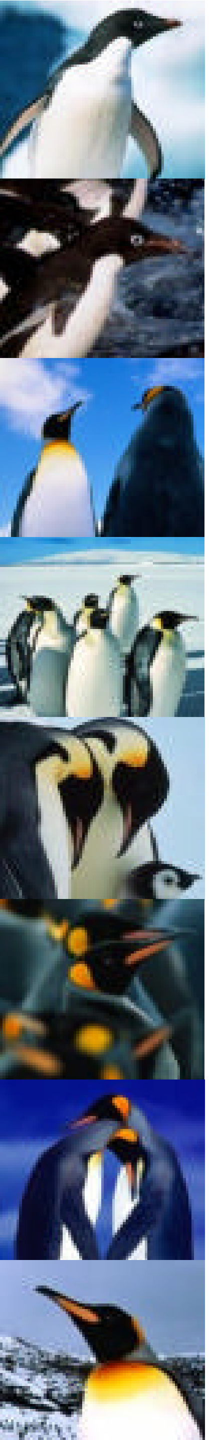
Does it work?

- Not with governments. Generally they insist on you paying them to carry out full source disclosure assisted verification – Open Source with a difference – before they will give an approval – approval by one nation does not always mean acceptance by another, except at very low evaluation levels. You should reflect on this.



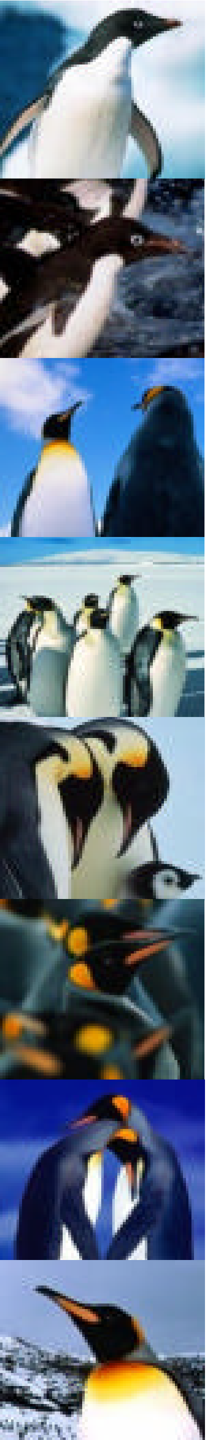
Any questions?

- Did you endorse Open Source?
- Should everyone use Open Source?
- Is Open Source one thing or a concept with many implementations?
- Has Open Group helped you understand Open Source?



Finally

Thank you for your attention



ARTICSOFT

Steve Mathews

CEO ArticSoft Limited

Tel: +44 (0) 871 871 0243
Fax: +44 (0) 870 011 7204
Mob:+44 (0)7   939 005 119