Exam Question

Ross Anderson

p7q3

Security part II – first question

Describe four of the problems from which classical multilevel-secure systems suffer.

(12 marks)

Your client is proposing to ~~use the information rights management mechanisms in~~ implement an email system with the property that every email sent internally within the company – that is, with no outside recipients – should be deleted after 180 days unless a manager authorises its retention.

Which of the above problems would you have to consider, and why?

(8 marks)

Model answer

First part is bookwork – 'Security Engineering' pp151-9 – composability, cascade, covert channels, upwards propagation of viruses, polyinstantiation, cost, TCB bloat, need to rewrite applications etc

Answer to second part depends on choices in first part. Composability could be an issue, if there are loops; cascade is unlikely to be, as we only have two levels; covert channels at the system level maybe not much, depending on the threat model; upwards propagation of viruses and polyinstantiation (qua cover stories) remain part of the environment; cost could be low with IRM/TC; TCB bloat is likely to be serious;

if

} if

~~2 eq {pop false}{pop HPwm begin HPwmEOP end} ifelse~~

end }

and the need to rewrite applications may not be an issue if you use Win2003 mechanisms (though there is then an issue of assurance).

The key point is that the email system described is classical MLS + timely destruction.