Security and trust for ubiquitous communication

J. W. Sanders

Programming Research Group, Oxford, UK

and

UNU-IIST, Macau

ITU WSIS Thematic Meeting on Cybersecurity

30 June 2005, Geneva

Security and trust for ubiquitous communication

Sadie Creese   Systems Assurance Group, QinetiQ, UK

Mike Reed   UNU–International Institute for Software Technology, Macau

Bill Roscoe, Jeff Sanders   Programming Research Group, Oxford, UK

1. The principle of distribution

2. A problem confronting software

3. Distributed authentication

4. Open source

5. Important problems

1. The principle of distribution

The purpose of ethical principles and
the problems with the normative principles Philosophy provides.

The principle of distribution.

Example from sport.

The principle's contributions to the five (?) modalities.

Examples of its application . . .

2. A problem confronting software

Types of software and the dynamics facing 'security software'.

Dynamics of security software; so specify its security conformance.

Compare with: software re-use.
Changing context; so specify its functional conformance.

Can the principle of distribution help?

Examples: propriety in the home; spam?; security?

3. Distributed authentication

The problem: bootstrapping authentication.

The appropriate model: modifying Dolev-Yao 1983
to allow empirical interaction.

Distributed protocols . . .

. . . and their formal proof and security conformance.

UK DTI's FORWARD project.

4. Open source

Shrink wrapped versus open source software:

centralised v. distributed: production/management/availability/ . . .

UNU-IIST's Open Computing Initiative.

Negroponte's $100-laptop project.

Functional conformance? Security conformance?

5. Important problems

1. Applying the principle of distribution:
   in which of the modalities?

2. Consider the idea of security conformance,
   investigate new and appropriate models of attack
   and classify software accordingly.

3. Invent protocols to keep pace with ubiquitous communication;
   and for changing control in times of crisis in a distributed
   system.

4. Open source meets (partially) centralised use;
   establishing its conformance?

   . . .   involving academia.