

Privacy and Security in the Information Society

Key findings from a UK-Japan symposium sponsored by the Engineering Academy of Japan and The Royal Academy of Engineering.

Held on 11-12 November at the British Embassy, Tokyo

Developments in information and communications technology (ICT) and the evolution of the 'information society' – a society in which ICT plays a key productive, economic and cultural role – have undoubtedly delivered widespread benefits. However, they have also brought to the fore questions and challenges for politicians, the public and engineers alike, such as how to strike the right balance between an individual's right to privacy and the state's duty to protect its citizens, and how to ensure that data is handled securely and used effectively and fairly. This symposium brought together leading engineers from Japan and the UK to discuss commonalities and differences between policy and perceptions in the two countries, explore the latest technological developments in the field, and identify questions that could usefully be addressed through collaboration between engineers in the two countries.

Policy

Participants from both countries agreed that the transition to the information society posed significant challenges in relation to privacy and security, which tended to differ from those in the physical domain. In addition, issues of privacy and security impacted directly on the relationships between individuals and society and employers and employees. Progress in technology and its uptake meant that increasing amounts of data were being collected, computers were often 'invisible' to the user and ICT was pervading society to a growing extent, all of which had implications for privacy and security.

It was considered important to recognise that attitudes and sensitivities towards privacy and security were not necessarily the same in the UK and Japan. Key concepts in Japanese society included 'Anzen' (safety) and 'Anshin' (sense of security), and the 'Uchi-Soto' model which was often used to characterise Japanese attitudes towards the self and others. The transition to an information society was thought to be having an impact on all of these. It was observed that the use of anonyms and pseudonyms in cyberspace was very popular amongst Japanese people (e.g. Japan has one of highest rates of anonymous editing in Wikipedia at 47%, compared with 30% in the UK and 19% in France), but concern remained over the younger generation's greater willingness to reveal personal data on the internet. In addition, while Japanese people had historically had a very strong sense of security, this appeared to be declining, particularly amongst the older generation.

In the UK, attitudes to privacy and security had been significantly influenced by high profile losses of sensitive data and the widespread coverage this had received in the media. While incidents of data loss and breaches of security were highlighted by both the UK and Japanese participants, the UK examples tended to involve the UK government and its agencies whereas the Japanese presenters focussed on incidents in the private sector. In contrast to the Japanese sense of security, fear of crime was a prominent factor influencing UK attitudes to security. This had in part driven the increased use of surveillance technologies in the UK, most notably closed-circuit television (CCTV) cameras. However, public concern was now mounting over the growth of surveillance and data collection in the UK.

These differences in attitudes between UK and Japanese citizens were also reflected in approaches to e-government. The Japanese government was in the process of developing and implementing ambitious plans for e-government, such as a personalised e-PO Box to control personal information flow between Japanese residents and the government. The more sceptical attitude of the UK public towards large-scale government ICT projects, perhaps reflecting past failures and greater sensitivity to potential risks, made such initiatives less likely to be supported in the UK. One potential challenge which applied to both countries, but which was particularly highlighted by the Japanese participants, was the need to promote and support uptake of these new electronic services by the older generation.

An area where both countries shared a common perspective was 'green computing'. It was agreed that there was a strong case for utilising technology to minimise the environmental impact of both computing itself and other activities. Examples included much more extensive use of sensor data to monitor and optimise transport networks, and utilising digital alternatives to physical activities e.g. virtual tourism. It was recognised, however, that the potential of green computing would only be realised if the associated dilemmas of security and privacy were acknowledged and resolved.

Another point of agreement between the two countries was the fact that the global nature of the internet meant that security and privacy challenges crossed national borders. At present, the necessary global governance structures and legal frameworks did not exist to enable these issues to be adequately addressed. Development of these structures would be a long term project but it was thought that academies could play a role in preparing the way.

Technology

Speakers from both countries addressed aspects of a range of authentication, identification and surveillance technologies, as well as the principles of software engineering which underpinned the development of secure applications. In particular, it was noted that privacy and security are aspects of dependability and, in addressing dependability, it was essential to be clear on the boundaries of the system being discussed. It was also observed that commercial software development typically resulted in quite high error rates which could compromise security, and dependability could never be demonstrated by testing alone. Instead, it was argued that the use of mathematically formal methods could overcome these problems and achieve dependability.

Radio-frequency identification (RFID) tags were the focus of much research and were expected to have widespread applications. Robust, ultra small, ultra-thin RFID chips (as small as 0.15x0.15mm²) could now be produced and developments had also enabled production of a double surface ultra small chip which could reduce assembly costs. Potential security applications included bank note counterfeit protection and document verification.

An additional topic of discussion was the potential for developments in image processing and pattern recognition to transform surveillance and security technologies. Improved automatic recognition of motion and unusual events could, for example, enable much more effective use of the data collected by CCTV.

It was also noted that developments in biometrics were increasing the range of possible applications for these technologies. Palm vein authentication technology was currently the leading biometric method in use in Japan (by market share).

Cryptography research in both Japan and the UK was addressing the need to provide high speed, low cost security for future mobile and ubiquitous applications, including for embedded devices such as DVD recorders and set-top boxes. Approaches from cryptography research were also now being applied to the development of hardware security.

Research questions

At the conclusion of the workshop, a discussion identified a number of open research questions stemming from the issues raised in the preceding presentations. These all concerned topics where joint or linked UK and Japanese research could be beneficial.

- How can the cultural differences between the UK and Japan be exploited to develop universally usable security approaches?
- What more can be learnt from the differences in attitudes towards privacy, security and ICT between the UK and Japan and how can this knowledge be applied to developments in technology and policy?
- How can the relative UK strengths in basic science and software and Japanese strengths in engineering and hardware be leveraged through collaboration in privacy and security research and development?
- How can ordinary users be persuaded to implement and utilise new security technologies?
- Can new security and privacy technologies be developed, or existing ones adapted, so that they are accessible and useful to the entire population, including disadvantaged groups such as the elderly and disabled?
- How can global governance structures be developed to enable issues of privacy and security in the digital domain to be addressed more effectively, and what role can engineering academies play in that process?
- Can Japanese and European governments co-operate to develop an open-source, provably dependable set of IT infrastructure components, so that it becomes economic to require that all systems that process personal data must be proved secure?
- Can developments in micro-RFID chips and RFID chips with embedded security be combined to produce ultra-small chips with embedded security?