European Security Standards Reference Implementation Initiative (ESSRII)

A Proposal for Action in Europe on International Information Security Standards

Brian Gladman, European Technical Director, Trusted Information Systems (UK) Limited.
Brian Randell, Department of Computing Science, University of Newcastle upon Tyne.

Purpose

The aim of this paper is to seek support for a co-operative initiative to ensure that European companies have early access to reference implementations of important information security standards being developed by international standards bodies such as The Open Group and the Internet Engineering Task Force.

Background

Over the past decade reference implementations of emerging software standards have played an important role in promoting their rapid transition from paper specifications to operational implementations within mainstream market products.

Internet standardisation bodies such as the IETF have relied heavily on experience gained in early prototype implementations to ensure that ratified standards are robust and effective. Moreover, as the benefits of open standards have become widely recognised, many companies have offered the results of their work, including reference implementations, for standardisation through international standardisation groups.

Such measures have generally been highly successful in promoting the rapid development of highly effective global information standards but in one area – information security – this process has run into difficulties.

The Problem

In recent years the rapidly growing importance of information security has led to the development of an increasing number of standards that involve cryptography. In this situation, when reference implementations have been provided they have become subject to export controls which have largely undermined their open exchange by the international development community.

For such standards the leading role of US companies in the information systems domain, when combined with US cryptographic export controls, has prevented non-US companies gaining early access to reference implementations. In consequence non-US companies have often found themselves at a severe disadvantage in exploiting important emerging standards in the information security field.

Although it can reasonably be argued that there is nothing to stop European companies building reference implementations in the security domain the fact is that this has not happened. There are probably a number of reasons for this:

- The relative weakness of European companies in the commodity software products market.
- The fragmented nature of the European information security market and its dominance by ‘nation by nation’ government interests.
- Hence a number of perceived constraints on open, pan-European co-operation in this field.

These difficulties must be overcome if Europe is to be able to ensure that its information infrastructures provide an effective and secure basis for the information society of the next century.

This paper looks at a small but significant step that could be taken to provide a basis on which to build European commercial strength in this vital area.

An Early Example

In the early 1990s the rapid growth of the Internet and the World Wide Web led to the introduction of the Secure Sockets Layer (SSL) standard as a basis for Web security. This standard, which made heavy use of public key cryptography, was initially promoted by Netscape who provided a reference implementation that was openly available within the US (and Canada). As a result of US export controls companies in Europe were unable to benefit from this early implementation and were hence at a significant disadvantage in attempting to take part in the development and evolution of this standard.

The result for Europe has not just been a further weakening of our software supplier base but also an undermining of the security available to European citizens when using the Internet and the World Wide Web.

Until recently almost all major Web server and browser products have been produced by US based companies such as Netscape and Microsoft. While US domestic versions of these products are available with strong cryptography, those available in Europe (and elsewhere) offer very limited cryptographic protection. Here the US government has used its export controls to ensure that the internationally available versions of these products have cryptography that is too weak to use for any serious purpose.

Cryptographic APIs

As a second example, in 1995 Microsoft published an interface standard – CryptoAPI™ – that would allow external cryptographic modules to be added to its 32 bit operating systems; that is to support ‘plug and play’ cryptography. However, in order to control the use of this interface, the US government insisted that Microsoft digitally sign any cryptographic modules in such a way that their operating systems would reject modules without correct signatures.

Within the US domestic market both the tools to use this interface and the signature process are not subject to government control and are hence available for general use. Outside the US, however, these capabilities are export controlled and the end result has been that non-US companies have been denied easy access to these capabilities. As far as is known to the authors, only one European company (and a subsidiary of a US company at that) has gained access to these facilities.

For the mainstream market, the ability to integrate cryptographic capabilities with Microsoft desktop operating systems is clearly very important. By constraining access by European companies to CryptoAPI™, the US government has created an unfair constraint on European self-determination in this vitally important area.

A Current Example

Recently Intel has released an innovative specification under the title ‘Common Data Security Architecture’ (CDSA). This standard provides a set of programming interfaces that allow secure applications to rely on a security management layer which integrates a set of underlying security functions. Detailed specifications for CDSA are available on the Intel Web site[1] This standard has been well thought out and promises to be influential in setting a standardised relationship secure applications and underlying security mechanisms.

[1] Details of the Intel ‘Common Data Security Architecture’ can be found at http://www.intel.com/ial/security/

While Intel has provided a prototype implementation of CDSA, because it involves cryptographic interfaces and cryptography, this is only available within the US and Canada. Again, therefore, we see an important emerging information security standard for which European companies are being put at a disadvantage because they cannot gain access to the implementations that are being used to underpin standardisation processes.

The strength of the CDSA is well illustrated by the fact that The Open Group has now unanimously adopted it as one of their public key management standards. This further underlines the importance of equality of access to reference implementations for such standards and illustrates the need for urgent action in Europe to prevent US export restrictions from undermining the interests of European companies in this area.

What Can Be Done

As already indicated, the fragmented nature of the European information systems market has meant that nearly all reference implementations have emerged in the US. This has not mattered outside the information security field since global access has normally been possible. However, when cryptography is involved access has been restricted and this has created a ‘non-level playing field’ as indicated earlier.

Although the costs of building a reference implementation can be significant – perhaps several man-years – at the same time they are not enormous. If a way could be found to share these costs across a large number of organisations, the costs to any individual organisation could be very small.

In practice, since the very intent of a reference implementation is that it should be openly shared in order to provide a spur towards rapid implementation, the idea of a pan-European co-operative initiative to provide reference implementations is well matched to this underlying principle.

This is the concept put forward in this paper – the idea of a co-operative university/industry partnership in Europe to develop and provide access to reference implementations of important international information security standards. The idea will be referred to here as the ‘European Security Standards Reference Implementation Initiative’ – ESSRII.

Organisation

There are many ways in which ESSRII could be organised. At one end of the scale it is possible that the development and provision of reference implementations in Europe could be commercially successful. In this model the reference implementations would simply be sold for profit. The problem with this, however, it that it requires a speculative investment and it is not clear whether this would be forthcoming. More importantly, however, this approach would not provide the ‘common ownership’ that is fundamental to the success of the reference implementation concept.

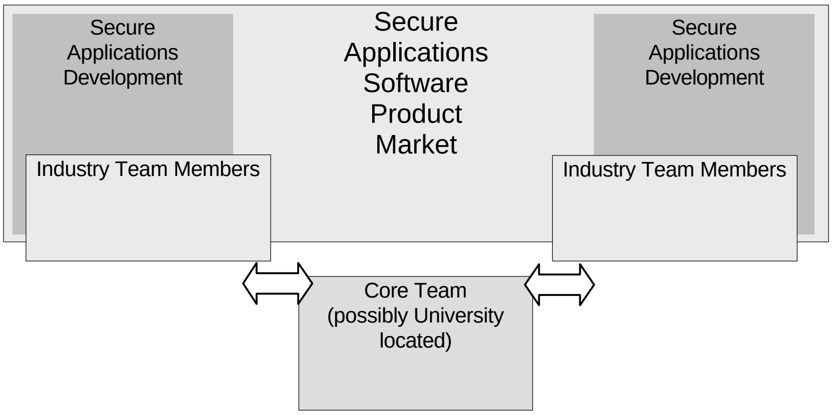
Another possible structure would be to form a group to undertake ESSRII that is funded by membership subscriptions. Subscribing members would get ‘free’ access to all results whereas other, non-member, companies would have to pay. The proceeds from the latter could be used to partly (or fully) sustain the operation. This model would go a long way towards meeting the need for ‘common ownership’.

Yet another possible approach would be for companies to contribute development effort into a distributed team. This would be more difficult to manage but would have the powerful advantage that the resulting reference implementations would have benefited from a broad base of knowledge and experience and a much closer coupling to those who will be exploiting them to produce commercial products.

In practice the last two options are not as different as they might seem. In the former arrangement it would certainly be true that company development teams would use the reference implementations as a basis for commercial product development and, in this sense, the model can be thought of as a distributed team with a 'core' component. Equally it is unlikely that the second model would work without a 'core' team of some kind.

Thus the most sensible organisation is likely to be a 'core' team together with resources made available by industry participants. The core team might be most appropriately located at a European University site (or sites). This would provide commercial neutrality whilst also allowing an appropriate University site to exploit and develop its related research efforts.

The associated industry groups could then be located in or close to product development teams, thereby providing a rapid exploitation route. There could also be secondments to and from the core team to provide for learning and experience transfer.


Secure Applications Development
Secure Applications Software Product Market
Secure Applications Development
Industry Team Members
Industry Team Members
Core Team (possibly University located)

The diagram above illustrates the organisational structure that looks most attractive for the proposed initiative.

Alternatives to a University location could be the augmentation of an existing industry research association or, possibly, an extension of the role of an existing standardisation group such as The Open Group, for example. The core team could be established by subscription from the industry members, by secondment of staff, or by a mixture of these or other possibilities. It might be possible to secure European Commission or European government funding for the initiative during its early evolution, and this would enhance its standing and greatly encourage European Industry to take advantage of its activities.

Access to Results

Open, unconstrained access to reference implementations is an important feature of their value and their success in rapidly moving standards into market products. It is thus vital that the model used to form ESSRII does not undermine such open access. At the same time, commercial investment in ESSRII is equally important if the initiative is to succeed and this means that a way has to be found to balance these objectives. One possible solution is that ESRII-produced reference implementations could be openly available for non-commercial use and free to ESRII members for their own commercial use. Commercial use could then be made available to non-members though licensing using terms agreed by members and any sponsoring bodies.

The need to ensure open access to reference implementations across European industry as a whole could be underpinned by securing public funding for the core team. This could be especially valuable in getting the initiative 'off the ground'.

Validation

If a reference implementation is to be truly useful there has to be considerable confidence in its correctness. Such confidence can be achieved in many different ways but one of the most important of these is continuing peer review of the evolving implementation. When compared with parallel and independent development of separate implementations, the development of a widely shared reference implementation will be naturally subject to a much higher level of scrutiny during its evolution. The breadth of contributions to its design and implementation will be such that refinements (errors) will be found more quickly and this will lead to rapid improvements in its robustness and effectiveness.

In addition, by locating the core team on one or more university sites, it will also be possible to build on the considerable software research strengths available in European universities. In the UK there are highly respected research teams working in the information security field at Newcastle and Cambridge Universities, and at University College and Royal Holloway College in London. Both at these sites and more widely in Europe there is much good work underway on the synthesis, analysis, design and verification of security protocols and standards, all of which could contribute significantly to the success of ESSRII.

In many respects, therefore, the proposal made here for pursuing ESSRII using a combination of a core team combined with distributed, industry-based resources will provide an effective basis for building robust and effective reference implementations which European companies could rapidly exploit in bringing software based security applications to market.

Such an approach not only reduces the costs to individual contributors but also provides the breadth of expertise and experience necessary to ensure that a sound and effective reference implementation emerges.

Getting Underway

In order to determine if the idea described here has merit it would be useful to see if it can be pursued using a practical, real world example of an emerging security standard. In fact an ideal opportunity now exists to do just this because there is to be a meeting in the UK in June between ICE and The Open Group at which co-operative possibilities in this general area will be discussed. In December last year The Open Group unanimously adopted the Intel CDSA standard and this could be an ideal first target for ESSRII action.

It is worth noting that CDSA contains similar cryptographic module digital signature requirements to those of the Microsoft CryptoAPI™. By taking early action to provide a reference implementation, organisations and companies in Europe will have direct control of (and access to) the module signature process and will not suffer the disadvantages that have become only too apparent in the Microsoft approach.

The Open Group has a strong track record in practical, effective and timely standardisation. The International Cryptography Initiative (ICE) has focussed its efforts on ‘Plug and Play’ cryptography standards, both at a technical level and in trying to achieve open, international access to such interface standards and the supporting technology. There is thus a good basis for co-operation between these two organisations in this area.

Initial Actions

This paper is being circulated prior to the meeting between The Open Group and ICE in June in order to ascertain the extent of the likely interest and support that it might receive. It is also being circulated to organisations that might be interested in hosting or participating in the ESSRII core team. Last but not least, organisations that might be prepared to offer support for the activity are also being approached. The aim will be to build on any feedback obtained in this process at the forthcoming meeting between The Open Group and ICE in June.

Conclusions

Reference implementations for standards associated with information security or cryptography often originate in the US and are hence not available to European companies because of US export controls.

If a way can be found to share the costs of such implementations across European industry, the costs to individual companies need not be large whilst the advantages will be substantial in terms of early access to practical implementation examples for important global information security standards.

This paper proposes a possible way of doing this – A European Security Standards Reference Implementation Initiative – that may prove attractive in Europe.

If there is sufficient interest this proposal will be discussed further at the forthcoming meeting between The Open Group and ICE to be held in the UK in June.