



Outsourcing or Insourcing software security??

The protection of software IP is as important for the small software developers as it is for the largest ones. With protection, developers will increase their profits by increasing revenue from paid usage. Generally developers lose out when their customers;

- *innocently* share software (eg in the office environment or at home),
- deliberately copy software or
- hack software as a result of the growing sophistication of the public in using the internet as a hacking resource.

This problem is equally true for both high and low cost software products. Many developers are unaware of the degree of piracy in the market place, choose to ignore this issue, simply feel too much effort is involved or are unaware of the new security tools available.

Some 34 per cent of the software installed on computers worldwide in 2004 was pirated, representing a loss of about US\$31 billion dollars to companies¹. Watch out if your market is Asia Pacific or Eastern Europe – piracy is running at 53% and 61% respectively.

With piracy estimates running at 34%, it is absurd that developers lose up to a third of their revenue due to the ignorance of the variety of protection that is available.

For those who choose to investigate this issue, the options are many. The choice of option comes down to three parameters for the developer.

1. The degree of risk of piracy
2. The possible solutions available
3. The effort and cost required for implementation.

This article focuses on parameter 2; the possible solutions available

Software Security can be approached in 3 ways;

1. Developed in-house
2. Purchased as a Software Development Kit (SDK)
3. Outsourced to specialist Security Service Providers

Developed In-House

Typically the security component of a software package starts out being a small ad-on module. Then, as the developers' software security knowledge matures, it is realized that real thought and real protection needs to be developed. By this time the investment to date makes it too costly or too embarrassing to change paths.

Unfortunately, by this stage, staff are distracted from roles requiring their core skills, or:

- additional programmers have been recruited and sent on security programming courses,
- additional infrastructure has been purchased such as authentication servers.
- significant change has been made to business processes.

As piracy becomes more sophisticated, these innovations need continuous upgrades and ongoing management, which will further deplete time and financial resources. There is no way of knowing how much investment is required since there is no way of knowing how many sales are being lost due to their poor security. A "Return On Investment" calculation is simply not possible.

¹ Second annual Business Software Alliance and IDC Global Software – Piracy Study May 05.

Software Development Kits (SDK)

An alternative to self-developed software security is to purchase a pre-packaged security code designed and written by specialists. A wide variety of SDKs can be found over the internet. Some only cost a few hundred dollars and provide a module for local activation (ie the software will decide to activate itself purely on whether an entered serial number matches a mathematical algorithm). More expensive solutions costing thousands of dollars, provide you with both client and server modules and in some cases hardware infrastructure for more holistic security – but this can be very costly. Here, their relationship with the software developer is essentially that of ‘commodity provider’.

Regardless of which SDK is purchased there is still the reliance on in-house resources to understand, integrate and support the delivered security into a product. Beyond this, there are further hidden risks that developers should consider.

These include:

- Limited Functionality – flexibility is not a feature common to SDKs. The customer facing-screen, the security message or response process may not be in keeping with the look or feel of the product being protected. Given the SDK is a generic package the supplier may be reluctant to create a variant which they would have to support on an ongoing basis. Even if they did, the cost to the developer may be disproportionate to the worth of the requested change making it impractical.
- Commonality – since the SDK is a commercially available product then there are most likely hundreds or potentially thousands of other products being protected in exactly the same way. If one product is hacked it is likely that others using the same system can also be easily hacked.

- Reliance – on the SDK company to quickly respond to queries, provide help, patches and upgrades. Since the relationship with the SDK supplier is transactional, it is very difficult to assess the level of support and how that may relate to problem management.

SDK's although useful, do not provide a total, flexible, customized management system.

Outsourced

Outsourcing is a strategy that allows management of software security to be maintained by experts in that field. These Services companies assist developers in all aspects of security. Unlike, an SDK provider, they seek to establish a long term relationship with the developer. Here, the Security Service Provider applies software protection to the developers' product and returns a protected version. The protection can be customized to the developers needs with many add on features if required. Data collection for Market Intelligence (MI) is one such feature providing reports which can be very useful for improving business and marketing strategies. MI includes:

- Monitoring the degree of piracy attempts
- Immediate notification of software registration for follow-up purposes.
- Confirming or assessing distributor's sales.
- Accurate quantitative data for profiling a customer base or market sector.

Certain elements of MI data can be leveraged to produce Business intelligence (BI) information. This is information distilled to the point where a direct (typically financial) benefit can be realised. For example, quantitative statistics about piracy attempts is MI that provides clarity over software usage. BI is where specific people or businesses can be targeted (ie contacted) and offered discounts on additional or bulk purchases of the software given the developer knows that



the target has tried and failed to use a copy of the software.

Another useful feature is full version trial software to "try before you buy". This allows true product evaluation of all features and function by the potential customer before purchasing. It increases the likelihood of a purchase while keeping development costs down. Here only one version of the product needs to be developed and maintained (ie a version that can securely operate in both demo and unrestricted mode). Also, the Security Service Provider uses economies of scale to keep infrastructure and support costs down.

Hence, the opportunity to outsource becomes a strategy in itself to keep costs down, maintain development schedules and attain the flexibility required to keep ahead of the market in terms of your product competition and in terms of piracy pervasiveness.

Notable international Outsourcing expert and lawyer Dr Trevor Nagel believes "when you're outsourcing, the wisest thing you can do is look for a solution rather than look for a specific technology". In other words:

- Identify your needs (eg piracy protection, activation capability, try-before-you-buy, Business Intelligence reporting, specialist infrastructure, expert security programmers etc)
- Look for a security services partner that can deliver your needs
- Let them worry about how to do it or what technology they will use

At the end of the day – and a day can be very short in the life of a pirated software product, it comes down to how open minded you are to the options. The more you retain in terms of control, expertise and infrastructure – the more it will cost you in time and money. At the other end of the scale, you must be prepared to give away some responsibility and control to establish a relationship with an expert provider that wants a long term relationship with you. Then you can focus on improving your product.

Regardless of whether you pull your head out of the sand or not, it will still be your product and you will still be accountable for its success.

Please don't hesitate to contact us should you wish to further explore these issues or provide feedback.

Saul Midler

saul@securewrap.net

Managing Director