WORLD FRAMEWORK FOR SECURITY BENCHMARK CHANGES

Lech J. Janczewski, Andrew M. Colarik
The University of Auckland, New Zealand

Abstract: The paper contains presentation of a framework, which would significantly increase quality of information security products and procedures, and Commentary on difficulties of implementing such a model. Main idea behind the framework is creation of a body assessing quality of information security products and procedures, similar to the system the ISO 9000 certificates.

Key words: Information security management, quality assurance, security benchmarks

1. CURRENT QUALITY ASSURANCE OF THE SECURITY PRODUCTS AND METHODS

Current quality assurance of the security products and methods could be divided into four stages:

Stage 1; A researcher / research facility announces a new product, which according to them, solves a specific security problem, for instance offering a new, more powerful cipher, new security protocol, etc. In most cases the product was released after passing in-house testing.

Stage 2; World community implements the invention, or product.

Stage 3; Other researchers start evaluation of the product and announce their findings through their publication channels. They usually are very eager to publish their findings as that such critique inevitably improves their standing within the security community. Hackers start the same activities but not all their findings are published. There are many “official” hacker publications, like “2600, the Hacker Quarterly” magazine (Hackers, 2002) or

hackers conventions, but in general, the knowledge is released to the wider community after they took advantage of their findings.

Stage 4; Upon receiving information about possible faults of the product the researches start developing mechanisms for blocking the discovered vulnerabilities of the systems. The process returns to stage 1.

What are the weak points of the process presented above? In our opinion there are several:

In the majority of cases, security products and procedures are not undergoing sufficient scrutiny of fellow researchers. Many software houses before releasing their products offer their product for free evaluation. However, the possible recipients of these packages are not in most cases chosen by their abilities to do a proper evaluation. There is no consistency with the critique of a new product. A publication with limited circulation could present the critique and the original developer would not have any opportunity to read it. Or even in the case of hackers, such critiques may never be published in a respected security forum.

Common Criteria are good as a presentation of general methodological assessment of the quality of security products but, for the obvious reasons, lacks details. Take for instance an issue of the physical protection of IT resources. It could be quite difficult to find direct instruction on how to evaluate system/devices falling into this category. Acceptance or rejection of a particular system could have significant financial consequences. The evaluation process should be set up in such a way that possible differences in the interpretation be eliminated to minimum.

2. MODEL CONCEPT OVERVIEW

There are three improvements to the above environment that we put forward.

1. The establishment of an independent, peer-based confirmation program that can validate specific capabilities and claims put forward by security vendors.

2. The creation of a certification program equivalent to Underwriters Laboratories (UL) and Canadian Standards Association (CSA) on products that carry liability insurance.

3. The establishment of security benchmark barriers for the purpose of disclosing the limitations of security products to the consumer similar in practice to Consumer Digest.

3. THE PROCESS

The validation/invalidation process consists of twelve (12) phases and is identified in the Table 1.

Table 1: Framework for security benchmark

Phase	Description
Classification	Apply a product to a classification system
Presentation	Apply standardized product presentation requirements to claims
Procedures	Develop revised verification procedures for each product based on original classification procedure
Validation	Product is submitted and evaluated by Verifiers
Reporting I	Initial reports generated by Verifiers - initial round
Reporting II	Exchanged reports allow re-examination by Verifiers
Final Report Generation	Reports are compiled and claims are validated/invalidated
Revised Claims	Manufacturer has opportunity to revise claims based on final report for certificate issuance
Certificate Issuance	Certificate is issued providing revised claims are consistent with final report
Certified Product Claims Published	Products invalidated by breaches may be revoked if not promptly addressed

4. ESTABLISHMENT OF SECURITY BENCHMARK BARRIERS

The first and second objectives are fulfilled through the validation and certification processes that have been outlined. However, as a security community of varying levels of expertise and understanding, there remains a need yet unfulfilled. The need is the dissemination of well-established issues about electronic security mechanisms. These issues are paramount to the establishment of procedures in the first and second objectives.

Authors, such as Bruce Schneier (2000), suggest that all security is based on social context and have identified fundamental weaknesses in the approaches to securing electronic based information systems. The Certification Granting Institution is positioned to accumulate and disseminate these fundamental concept weaknesses to all the Players. This is the first logical step in focusing developmental efforts by the security community for the improvement of the industry. It would also serve to educate a realistic approach by consumers for the implementation and maintenance of security within their respective organizations.

The final question is: which organisation should participate in the process, or rather, which organisation should be appointed as having rights to issue certificates and perform the validation tests? We think that the reverse question may be a bit more appropriate: which organisations should not play these roles? In the case of testing facilities, they should not be connected with any manufacturer of security products. That would eliminate claims of possible bias in their opinions and findings. On the other hand, the certificate granting bodies should have international recognition.

Many national standards organisations are issuing the ISO 9000 certificates. The verification process leading to ISO certificate issuance is carried out by the standard organisations themselves. Hence the national standards organisation could be a good candidate for issuing such certificates. Other possible candidates could be CERT-type centres or units attached to such bodies as TC-11 of IFIP.

5. CONCLUSIONS

Annual CSI/FBI (2002) report on status of the information security affairs clearly indicate that loses resulting from abusing information systems are on a constant rise. This indicates that despite all the claims the security industry is still behind the attackers. This is reflected in public perception that conducting business on Internet is not secure.

If that trend is to be reverse, the security industry must undertake some drastic measures to increase the quality of its services and products. We believe that the path we have outlined in this paper is a right way to go. We do not claim that this is the only way to solve the problem, but we think that the security industry must establish a testing and certification environment for their products and services in a trusted third party manner.

REFERENCES

Hackers, 2002, *2600, the Hacker Quarterly*, http://www.2600.com

Schneier, B., Fixing Network Security by Hacking the Business Climate, proceedings of the IIR 7th proceedings of the IIR 7th Annual National Summit on IT Security, 2002

CSI/FBI Computer Crime and Security Survey, http://www.gocsi.com/press/20020407.html, 2002

Schneier, B., Secret & Lies, Wiley, 2000