SIV Workshop Position Paper
VoiceXML SIV Security

Speaker Identification and Verification (SIV) is a crucial component of iBiometrics products and services. iBiometrics, Inc. (iBiometrics) is interested in the success of SIV in evolving standards. To advance SIV standards, iBiometrics has participated in the VoiceXML Biosig committee for the past several years and contributed to its efforts. Participation in the workshop builds upon gained knowledge and is a continued effort to advance SIV and related standards.

There are a number of potential important topics for a position paper including SIV security and SIV integration with distributed and centralized identity management frameworks. It is iBiometrics viewpoint that the highest priority is that SIV, related standards and applications are secure. The business and regulatory community are aware of the high cost of insecure applications given the explosion of exploited software vulnerabilities over the past five years. Software quality assurances and security mandates are becoming common place. For example, recently, the US Federal regulatory environment has expanded to address the requirement for ongoing, measurable software security assurance programs. Agencies must now demonstrate their compliance. Both FISMA and DITSCAP/DIACAP dictate that risk assessments of critical applications be performed periodically to determine potential exploits, and require the remediation of uncovered flaws (1).

iBiometrics recommends that the W3C initiate a security project or projects in conjunction with the VoiceXML organization and other supporting organizations that address VoiceXML 3.0, SIV and other W3C related standards and application security. This proposed effort will increase adoption of these standards because, as stated above, organizations will be able to understand the risks and costs prior to implementation of platforms and applications. It is well known that rework to address software design and coding flaws is highly costly. Capers Jones, one of the driving forces in the field of software estimation, describes these costs in detail in his book, Estimating Software Costs (2) where he states that defect repair costs and schedules are often larger than coding costs and schedules. It is essential to the success of SIV that the standard is security and the standards it relies on are secure so that adopters who follow application security and SIV best practices will be able to cost effectively implement new applications.

VoiceXML 3.0 and the associated W3C standards are designed to add significant functionality in addition to SIV as described in the December 2008 W3C working draft. Despite the separation of the data, flow and presentation layers, the overall complexity increases significantly. Increased functionality and complexity means increased vulnerabilities. iBiometrics recommends that the proposed project(s) utilize established security methodology. This position paper references the Addison-Wesley Software Security Series of books by world authority of software security, Gary McGraw, PhD (2) to illustrate and substantiate its position. In his book, Software Security, Building Security In, Gary McGraw looks to solve the security challenge through a three pillar approach; applied risk management, software security touch points and knowledge.

Risk Management

Security practitioners recognize the fundamental point that security is risk management. Risk management is an iterative risk identification and mitigation approach that is deeply integrated throughout the software development lifecycle (SDLC). The proposed development of a risk management framework for VoiceXML, SIV and other related standards would enable the standards organization to identify, rank, track, and understand software security risk as the touchpoints are applied throughout the SDLC. This effort should include VoiceXML and SIV architectural risk analysis which applies risk analysis techniques while the software standard is being designed and built.

Security Touchpoints

Practitioners are increasingly incorporating software security best practices in their work. The software security touchpoints involves applying engineering lessons throughout the development process. The security project proposes applying the touchpoints throughout the SDLC for the VoiceXML and SIV standards and applications. Applying touchpoints throughout the SDLC will decrease unidentified design and code flaws.

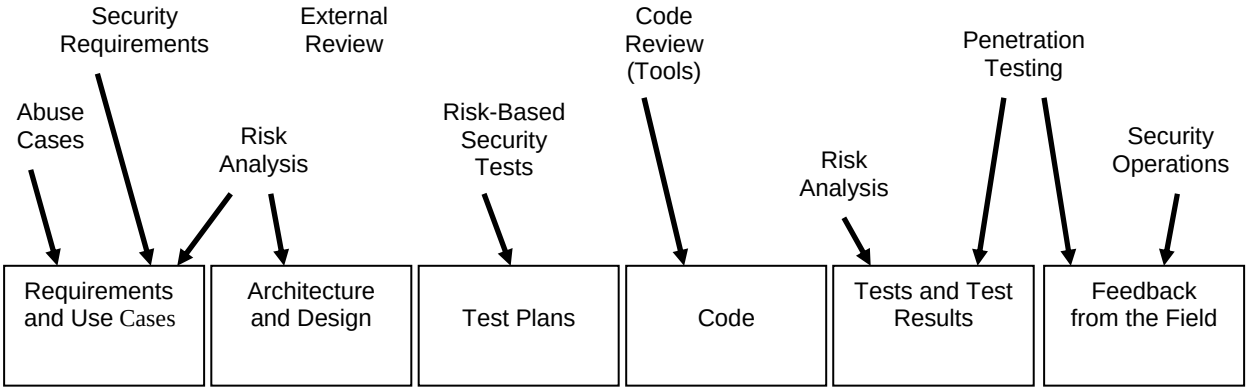

Figure 1: Security touchpoints throughout the Software Development Lifecycle (SDLC)

Knowledge

It is important to build knowledge and experience within the community. Gary McGraw notes that knowledge is information in context. For example, it is not just a general list of coding vulnerabilities but the same information built into a tool for VoiceXML SIV static code analysis. Knowledge can be organized as **principles, guidelines, rules, vulnerabilities, exploits, attack patterns, and historical risks.** This highly useful knowledge can in turn be organized into prescriptive, diagnostic and historical knowledge. The proposed security project(s) builds knowledge for use specifically in the VoiceXML software development community so that secure SIV applications are readily attainable. A tangible example of a knowledge deliverable to date by the SIV biosig committee is the initiated SIV best practices effort.

In summary, the paper proposes applying established and successful software security approach to VoiceXML, SIV and other related standards and applications. This security effort will facilitate secure, cost effective and compliant standards and VoiceXML SIV applications.

References

1. '**Software Security Assurance',** Compliance Guide for Federal Agencies, Library of Ounce Labs, http://www.ouncelabs.com/abstracts/Software_Security_Assurance_fed.asp

2. '**Estimating Software Costs, Bringing Realism to Estimating'**, Caper Jones, MacGraw-Hill, 2007.

3. '**Software Security, Building Security In'**, Gary McGraw, Addison-Wesley, 2007