AVDL Application Vulnerability Description Language

Frequently Asked Questions

Application Vulnerability Description Language (AVDL)

What is AVDL?

The Application Vulnerability Description Language (AVDL) is a new security interoperability standard being proposed by leading application security vendors as part of the OASIS standards process. The goal of AVDL is to create a uniform way of describing application security vulnerabilities using XML.

What is the business problem AVDL is addressing?

AVDL will address the business problem of how companies manage ongoing application security risk on a day-to-day basis. Application security, by definition, is far more complex than network security. To begin with, each application is entirely unique. With the wide adoption of web-based technologies, applications have also become far more dynamic, often changing daily, or even hourly. To make matters worse, enterprises must deal with a constant flood of new security patches from their application and infrastructure vendors.

To address this growing problem, companies have begun deploying best-of-breed security products to discover application vulnerabilities, block application-layer attacks, repair vulnerable web sites, distribute patches and manage security events. Unfortunately, there is currently no standard way for these products to communicate with each other, making the overall security management process far too manual and time-consuming.

What is needed to solve this problem?

We are proposing the creation of a standard XML description language to define, categorize and classify application vulnerabilities in a way that can be understood and used by a variety of security products throughout the application security lifecycle. Assessment tools, for example, could create an AVDL file for a particular application that could be read by attack prevention products to recommend the optimal policy for that specific application. Remediation products could use AVDL files to suggest the best course of action for correcting problems, while reporting tools could use AVDL to correlate event logs with areas of known vulnerability. This interoperability will make it far easier for security administrators to manage risk in a constantly changing environment.

How will this benefit customers?

During the application development and testing phases, AVDL will serve as a standard language used by developers and QA testers to identify and remediate pre-production security issues. Finding and correcting security defects early in the application lifecycle is a proven method of overall cost reduction. During the production phase, AVDL will improve the effectiveness of application security gateways through extended rules based on better definition of existing vulnerabilities. It will also serve as a consistent communication mechanism to improve the vulnerability reporting process and appropriate vulnerability remediation. In post production, auditors will spend less time understanding various reports from disparate sources and more time documenting their findings. Ultimately, customers will benefit from both reduced application security risk and decreased total cost of operations and ownership.

Who are the companies proposing AVDL?
The AVDL proposal is being made by five product vendors, representing various aspects of the Full Application Security Lifecycle. In alphabetical order, these companies include:

- Citadel, security remediation
- GuardedNet, security event management
- NetContinuum, application attack prevention and secure application access (co chair, AVDL TC)
- SPI Dynamics, application vulnerability assessment (co-chair, AVDL TC)
- Teros, application attack prevention

Why are these companies proposing the AVDL standard?
The proposing companies each manufacture products that focus on specific areas of the application security lifecycle. Enterprise customers are asking all of these companies (and others) to provide products that interoperate. A consistent definition of application security vulnerabilities is a significant step towards that goal. Today, these vendors are actively engaged in a project whereby XML-based vulnerability assessment output will be used to improve the effectiveness of attack prevention, event correlation, and remediation technologies. XML establishes a common framework, but XML alone does not ensure vendor interoperability. In fact, the first implementation of these XML-based information exchanges will be proprietary, as no suitable standard exists. We believe that customers should ultimately be given the benefit of interoperability between all vendors in each category of the application security lifecycle, allowing them to select those products that offer the most useful functionality for their unique and individual requirements. As a vendor neutral open forum, OASIS is an ideal vehicle for pursuit of this goal.

What types of companies will contribute to the formation of AVDL?
All members of OASIS are invited to help craft the AVDL specification. We anticipate active participation from leading vendors, integrators and enterprises with expertise in the technologies and real-world business problems of managing application security.

- **Examples of how application attack prevention products will use AVDL.** Application attack prevention products operate much like firewalls for the web data center. They typically sit in front of web applications, performing deep inspection of all incoming requests, blocking application-layer attacks that traditional network firewalls can’t protect against. AVDL will make it easier for attack prevention products to recommend optimal policy settings based on vulnerabilities discovered by assessment tools or attack activity reported by event management systems. Using AVDL, the output of periodic vulnerability assessments could also be read directly by attack prevention products, ensuring up-to-date protection on an ongoing basis.

- **Examples of how application vulnerability assessment products will use AVDL.**
  Application vulnerability assessment products typically identify vulnerabilities, rank them by severity level, and provide detailed remediation information. These products identify and prioritize issues, but they don't solve problems. Security administrators still have to figure out how to take these suggestions and actually implement the recommended solutions. With AVDL, a standard form of communication will exist whereby vulnerability assessment tools will be able to describe, in great detail, the state of application vulnerabilities at any point in time. Multiple vulnerability assessment tools could then be used by one enterprise, as AVDL will support quick distillation of output into one consolidated source. This information will be used to improve the effectiveness of attack prevention products, to increase the success rate and effectiveness of remediation tools, and to further enhance the value of event management and reporting tools by providing important additional information to operations and management personnel.

- **Examples of how remediation products will use AVDL**
  Remediation products are dependent on two vital types of information: They must understand where the vulnerabilities are and they must know what fixes are required. Remediation products may rely on outside sources to provide much of this information, particularly information related to the actual discovery of vulnerabilities. This is certainly true regarding application security vulnerabilities. Using AVDL, remediation products will be able to process an XML-based input stream that describes existing application vulnerabilities and the required corrective actions, then use that information to effect automated patches when appropriate. When vulnerabilities are corrected, remediation products could also use AVDL to communicate this information back to the attack prevention gateway protecting the site so that its policies could be modified accordingly.

- **Examples of how security event management products will use AVDL**
  Security event management products address a common problem: Security administrators are required to process an inordinate amount of input from various sources and are then expected to focus on the issues that require immediate attention. In most organizations, and in virtually all large enterprises, these administrators are overwhelmed with sensory data. The objective of an event management product is to gather all of the data, apply a set of rules and policies against that data, and to prioritize information so that the administrators can truly focus on the areas of highest impact. The more information that an event management product can process, the better the results. AVDL will provide a standard vehicle for communication of existing application security vulnerabilities, their severity and their potential impact on the organization. As a result, event management products will be able to more efficiently correlate application security vulnerabilities with actual security events, making it easier to prioritize remediation activities and set policies in attack prevention gateways.

- **Examples of how dev tools, app servers, ERP vendors, auditors use AVDL**
  As a standard format for application vulnerability descriptions, AVDL will be used by many other products throughout the application security lifecycle. Using AVDL as an input, for example, development tools will be able to include this information within "standard" reports during the development phase. ERP vendors could use AVDL as a format to communicate potentially vulnerable configurations, making it easier for customers to ensure secure deployments that fit their unique environments. Auditors could use AVDL output from assessments as input to reports that track trend analysis and compliance.

Will ADVL only address application vulnerabilities?
Yes. While network-layer attacks are obviously important, the primary focus of AVDL is to provide a common way to describe application vulnerabilities.

Will AVDL address viruses and worms?
Internet worms like Code Red, Nimda and SQL Slammer that attack vulnerabilities in web sites clearly fall within the scope of AVDL. The AVDL charter does not, however, attempt to address traditional viruses.

Will AVDL address XML-based web services?
We fully expect XML web services standards like SOAP to play a key role in application-layer vulnerabilities going forward. As such, this definitely falls within the scope of AVDL.

Why did you choose OASIS?
OASIS is a highly credible global consortium comprised of over 600 corporate and individual members designed exclusively to drive the development, convergence and adoption of e-business standards. The OASIS process has proven extremely successful in fostering the creation of worldwide standards for security, web services, XML conformance, business transactions and web interoperability. As such, we believe it is the ideal forum to help us produce a timely AVDL standard that will benefit organizations of every size and industry affiliation.

Who can participate in helping to define AVDL?
Any OASIS member with interest in solving this problem is welcome to join the AVDL Technical Committee.

When will the first AVDL specification be completed?
The first meeting of the full OASIS Technical Committee for AVDL has been scheduled for May 15, 2003. The first candidate AVDL specification will be posted for comment by Q3 of 2003 with a final AVDL 1.0 specification posted by Q4 of 2003.

How is AVDL Different From Efforts Like CVE and VulnXML?

AVDL is not intended to duplicate or replace any existing industry standard and should be entirely complimentary to efforts like CVE and VulnXML. Both CVE and VulnXML focus on creating more uniform ways for security researchers to describe and classify specific new vulnerabilities when they are initially discovered in much the same way anti-virus researchers have been attempting to do for years. CVE is valuable primarily for describing and classifying network-layer vulnerabilities, while VulnXML attempts to add some of the detail needed to adequately describe application-layer vulnerabilities. The vendors proposing AVDL support both CVE and VulnXML.

We are proposing AVDL to address the broader business-oriented problem of how companies actually manage ongoing application security risk on a day-to-day basis. Managing application security risk in a highly dynamic environment can be an extraordinary challenge for security administrators. Fortunately, there are now a wide variety of best-of-breed products on the market to help companies with the task of discovering application vulnerabilities, blocking application-layer attacks, repairing vulnerable web sites, distributing patches and managing security events. Unfortunately, these products have no universal way to communicate with each other, making pragmatic management of this risk a highly manual, and often complex, process.

The goal of AVDL is to help companies begin managing the Full Application Security Lifecycle by providing a more uniform way of communicating application security vulnerabilities, policies and events via XML. It is the full intent of the vendors proposing AVDL to repurpose any positive progress that has already been made by the security community to date.

Where can I find more information about AVDL?

More information about AVDL can be found on the Oasis web site at http://www.oasis-open.org, or the AVDL informational site at http://www.avdl.org/.