Chris Vanden Berghe <vbc@zurich.ibm.com> on 04/18/2005 05:05:12 PM

To: submissions@nspw.org
cc: James Riordan <rij@zurich.ibm.com>
Subject: research paper submission: A Vulnerability Taxonomy Methodology applied to Web Services

Please find our submission for the NSPW attached. One of the authors, namely Chris Vanden Berghe, will gladly attend the workshop.

Our justification for inclusion in the research track of NSPW:

We think that the paper "A Vulnerability Taxonomy Methodology applied to Web Services" is well suited in the category "Research Paper" for the NSPW as it is a first step in what seems to be a very promising direction rather than a variation or improvement in an existing body of work.

The paper has two parts: the first develops a methodology to capture and formalize the intuition that allows security professionals to make predictions about likely security problems and the second applies the methodology to web services (WS). We find that the second part practically validates the first in that the application yielded both anticipated and unanticipated, yet retrospectively clear, results.

The former class includes the high likelihood of input-validation problems and introduces concrete examples of new attacks that are evolved from old (such as XPath injection as a WS evolution of SQL injection). The latter class includes the high likelihood of the WS architecture to pass attacks onto back-end components as well as the notion of attack flows which challenges the obvious roles of attacker and victim.

We think that both parts could benefit from the workshop environment offered by NSPW. Regarding the methodology itself, our goals were quite practical and so we were reassured by the anticipated results and pleased with the unanticipated. Nonetheless, we would like to solidify the validation of the methodology and, in so far as we are trying to capture and formalize security intuition, we think that interactive discussion with a diverse collection of security professionals would help drive the work to maturity and wider utility. Regarding the

application of the methodology to web services we are interested in those areas where the collective security backgrounds of the NSPW participants cover areas not captured by the authors' particular security backgrounds and may therefore not be captured in our model.

Best regards,

James Riordan and Chris Vanden Berghe.

- A_Vulnerability_Taxonomy_Methodology_applied_to_Web_Services.pdf

We think that the paper "A Vulnerability Taxonomy Methodology applied to Web Services" is well suited in the category "Research Paper" for the NSPW as it is a first step in what seems to be a very promising direction rather than a variation or improvement in an existing body of work. The paper has two parts: the first develops a methodology to capture and formalize the intuition that allows security professionals to make predictions about likely security problems and the second applies the methodology to web services (WS). We find that the second part practically validates the first in that the application yielded both anticipated and unanticipated, yet retrospectively clear, results. The former class includes the high likelihood of input-validation problems and introduces concrete examples of new attacks that are evolved from old (such as XPath injection as a WS evolution of SQL injection). The latter class includes the high likelihood of the WS architecture to pass attacks onto back-end components as well as the notion of attack flows which challenges the obvious roles of attacker and victim. We think that both parts could benefit from the workshop environment offered by NSPW. Regarding the methodology itself, our goals were quite practical and so we were reassured by the anticipated results and pleased with the unanticipated. Nonetheless, we would like to solidify the validation of the methodology and, in so far as we are trying to capture and formalize security intuition, we think that interactive discussion with a diverse collection of security professionals would help drive the work to maturity and wider utility. Regarding the application of the methodology to web services we are interested in those areas where the collective security backgrounds of the NSPW participants cover areas not captured by the authors' particular security backgrounds and may therefore not be captured in our model.