Secure Web Applications & Web Services Architectures

Wednesday 2 March 2005 (14-21h), Hotel Sofitel Brussels Airport (Diegem)

This seminar is organised in cooperation with Ascure (www.ascure.com)

Full Programme

13.30h-14h: **Registration and Coffee/Tea**

14.00h: An Intro into the Most Common Threats for Web Applications (Jan De Meyer, Ascure)

Web applications are omni-present, but few people seem to understand to what a degree those applications can expose their environment. In this introductory session we will try to give you an insight why almost 80% of the hacks today involve web-application hacking. We will take you conceptually through a number of scenarios which might expose your data and/or your organisation.

- Network- and System-level attacks: your infrastructure and entry points through the eyes of an attacker ("hacking inside-out")
- Specific web-attacks: hidden field manipulation, cookie poisoning, backdoor & debug options, application buffer overflow, stealth commanding, 3rd party misconfigurations, known vulnerabilities, parameter tampering, cross site scripting, forceful browsing, SQL injection, ...

14.50h: The Architectural Building Blocks of Secure e-Architectures (Erik van Zuuren, Ascure)

Once your risks and required controls are known, things need to be put in place. And as security is determined by the weakest link, this session will look at all architectural and procedural elements you should have in place if you want to have a trust-worthy environment. We will give you a good insight into what concepts like multi-layer defence and time-based security really means and why you need to have those in mind.

- Risk management aspects: applying frameworks, baselines and risk management techniques to Web application and Web services environments
- Layered Security Aspects: Network-layer controls, System-Layer Controls, Application-Layer Controls, etc. Understanding the (in)abilities of firewalls, application-level firewalls, intrusion detection, anti-virus, ...
- Policies-elements and Crucial Processes: Personnel Security, Physical & Environmental Security, Communications and Operations Management, Access Control, Systems Development and Maintenance, Compliance, ISO 17799, ...

15.40h: **Coffee/Tea and Refreshments**

16.10h: Web Applications: Secure Development Guidelines and Principles (Sebastien Deleersnyder, Ascure)

As becomes clear over and over again: the development department needs to work under severe time constraints, constantly changing requirements, ever-evolving technical evolutions, ... and worst of all without any clear principles or guidelines on how to deliver secure applications. In this session, we therefore want to give you some insight on what your development department should know and how things could be put under control methodologically.

- Some rules and techniques (at conceptual level):
  - Validate input and output
  - Fail securely
  - Make it simple
  - Use and reuse trusted components
  - Defense in depth
  - Only as secure as the weakest link
  - No security by obscurity
  - Least privilege
  - Compartimentalization
  - Trust no one
  - Input validation
  - Stored procedures
  - Session management

This seminar is organised in cooperation with Ascure (www.ascure.com)

17.00h: Web Application Firewalls: Mitigating Risk & Buying Critical Time (Jan De Meyer, Ascure)

Even with the best of guidelines, even with the best procedures, things sometimes go wrong, or required changes can not be executed due to conflicts with the production environment. What do you do if the alarm goes off but your hands are tied ? This session explains how Web application firewalls can buy you critical time and what their impact is on your environment.

- An overview of mitigating solutions in the market place.
- Understand how Web application firewalls work and buy you time
- Where to put Web application firewalls and the possible consequences
- Creating rules and tuning Web application firewalls
- What (and what not) to log

17.50h: **Dinner**

19.00h: Important Cornerstone: Identity and Access Control Management (Erik van Zuuren, Ascure)

Even the best of controls can not function properly if you haven't got a clue who is doing what, where and when. Identities, roles and privileges must be uniquely determined and stringently administered. This session will take you through the most important aspects of identity management, role- and privilege-based access. Also, you will get some insights into different federation models and what can or can not work. Finally as identities in the Web services world are no different from identities in the Web application world, we will give you some ideas on how to keep both worlds in sync.

- The building blocks of IAM in a web-context
- Identity Management and Provisioning issues
- Successful Access Management strategies
- Authentication-, Assertion- and PKI-integration specifics
- Delegated administration versus Federation

19.50h: The (immediate) future: Web Services and their Security Aspects (Sebastien Deleersnyder, Ascure)

Web services are not only rapidly becoming a cornerstone in backend connectivity and enterprise application integration (EAI), but they are also about to cause the same evolution boom as Web applications did. Regrettably, few of the Web services already in production have true security on board. Partly, because it is just standardizing. This presentation will give you a look ahead on how to successfully protect your Web services.

- Web services: already in more places then you would think.
- Web services security models and features (WSTrust, WSS, SAML, ...)
- Which features to use when and where ?
- Integration of IAM and Web services

20.40h: **Conclusions & Summary / Final Q&A**

21.00h: **End of the Seminar**

Secure Web Applications & Web Services Architectures

Wednesday 2 March 2005 (14-21h), Hotel Sofitel Brussels Airport (Diegem)

Goals of this Seminar

Web Applications have become the point of entry to critical and confidential data, and have become the interface to internal resources, e-business and e-government platforms. Yet, ***we read time-and-time again that important data has been exposed and compromised via insecure Web applications***.

Web Services may not be really visible, but there are more and more of them everyday. They ***are being set up both internally*** within organisations to facilitate internal communications and processes, ***and externally*** to facilitate the exchange of business-critical (e.g. financial) data. ***Most of these Web Services lack any solid security***.

Everyone is using these technologies to unlock data and processes, even over the Internet. The advantages of being able to flexibly reach anyone, anywhere, anytime are clear. However, it is important to ***only unlock wisely and in a controlled and secure fashion***.

This seminar will give a good insight in these topics. It will refrain from being highly technical and try to ***run you conceptually through the different topics*** which should be looked at when setting up any Web Application or Web Services Architecture.

First of all, we will set the scene using some simple examples of ***how Web resources can and are easily exploited***. Then, we will give a complete overview of the scene and ***all procedural and technical controls to mitigate these risks***.

Secondly, we will get into Web application security specifics: ***how should Web applications be securely developed*** and what extra layer of security can be put in place to mitigate human/programmer's failure ?

Next, we will add and discuss ***identity and access control management*** as an important component, and show how this best fits into Web environments.

Finally, we will look at ***Web services***, their specific security issues and how the lessons we already learned can be re-applied to these Web services.

This seminar is organised in cooperation with Ascure (www.ascure.com)

Speakers at this Seminar:

Jan De Meyer is a Senior-level Information Security Consultant at ***Ascure*** with extensive experience in designing web-architectures and securing Windows environments. In 1998 he started specializing in security with a primary focus on Microsoft-based solutions. The last 4 years he extended his specialization with ***securing web-based applications for a wide ranges of industries*** (banks, hospitals, pharma, ...), and ***he actually implements those complex architectures as well*** (Portals, Load-Balancers, reverse proxies, ...). Besides technical certifications (MCSE, RSA, Sanctum,...) he obtained both the CISSP and CISM certification.

ir. ***Erik R. van Zuuren*** MBA stepped into ICT some 10 years ago and into ICT-consultancy some 8 years ago. Erik now is a Senior Information Security Consultant at and Business Development Manager for ***Ascure NV/BV***. He assisted to several CIO/CTO/CISO's and coached several InfoSec- and ICT-security projects as well as organisational embedding programs. He ***creates security strategies, frameworks and environments for medium/large organisations and government agencies***. He also creates Identity and Access Control Management as well as Public Key Infrastructure blueprints, concepts and architectures. He ***coaches the Flemish Government in their process/application PKI-enabling-roadmap for strong authentication, access control management and digital signatures***, and was one of the authors/fathers of the blueprint for the Belgian Personal Identity Card Project (BelPIC) and of the Belgian Federal PKI program.

Sebastien Deleersnyder is a Senior-level consultant at Ascure with ***extensive experience in security-related disciplines, both at strategic and tactical level***. He implemented more general security products, such as firewalls, IDS and content technology, he revised and advised upon security architectures for the banking and insurance sector, and he performed security audits and performed the role of Security Officer for projects of the European Commission. ***He specializes in (Web) application security combining both his extensive development and information security experience***. Sebastien holds a Master in Informatics, and is a CISSP, CISM, and PRINCE2 certified project manager.

Questions to be Answered:

- How can Web resources be exploited (= abused) ?
- How do I assess risks ?
- What are the generic (not application-specific) building blocks to secure my environment ?
- What are the development guidelines and principles for secure Web applications, and how do I mitigate human/programmer's failure ?
- How does Identity and Access control fit in ?
- What are the security aspects of Web services and service-oriented architectures ?

Price of this Seminar:

The price of this seminar is ***480 EUR (+ 21 % VAT)***, incl. participation to the seminar, handouts, dinner, coffee/tea, and a lot of background information on the development of secure Web applications and secure Web services architectures.

Discounts:

For ***simultaneous registrations (one invoice)***, the 2nd participant of the same company receives ***10 %***, the 3rd ***20 %*** and all further participants ***30 % discount***. A 20 % discount is given to participants from schools and universities.

Cancellation:

Cancellation is possible up to 1 week before the seminar, if received in writing. In this case, 20 % of the total amount is charged for administration. Otherwise, the full registration fee is due, ***regardless of the reason of cancellation***. Of course, ***replacement*** is possible at no extra charge.

Who Should Attend ?

- ***"Business-side" people*** who want to understand what security controls and assurances they can and should demand in e-business, e-gov and e-services projects.
- ***"IT-side" people*** who need to know the measures to secure their IT-services/architectures.
- ***Security people*** who have to guide and guard the process and the security solutions.

Registration Form

Fax to: (09) 241.56.56 or backup fax (09) 220.34.57 - Questions ? Call (09) 241.56.13 or e-mail seminars@itworks.be

Your data will be recorded in the database of I.T. Works bvba, so that we can keep you informed about our activities. In accordance with the law of 8/12/1992 on the protection of privacy, you can inspect and, if necessary, correct this data.

❑ Mr. / ❑ Mrs.

Name: ________________ First Name: __________

Job Title: ______________________________________

Company: ______________________________________

Company Address: ______________________________

____

Phone: ________________ Fax: ______________

VAT/BTW/TVA nr.: ______________________________

E-Mail: _______________________________________

Agrees with the seminar conditions, and registers for:

Secure Web Applications and Web Services Arch. (2 March)

Please send the invoice for 480 EUR (+21% VAT) to my

❑ Company address
❑ Personal address: __________________________

Extra info for invoice (like order nr.):__________________

Date _____________ Signature ________________

Please complete and return this form by mail or fax to: *I.T. Works, Innovation Center, Technologiepark 3, 9052 Gent,* ***fax: (09) 241.56.56*** *or* ***(09) 220.34.57****. After receipt of the registration form, you will automatically receive a confirmation, invoice and a detailed access plan.*