RSA CONFERENCE 2008

Call for Speakers Offline Submission Form

SESSION INFORMATION

* = required input

- **Session Title *** (Limit 75 characters)

  High-Speed Risks in 802.11n Networks

- **Session Abstract *** (Limit 400 characters including spaces)

  The latest excitement in WLANs is the promise of 100 Mbps connectivity with IEEE 802.11n. While many organizations seek pre-N solutions or plan to deploy ratified 802.11n neworks in the future, few are considering the security implications of this technology. This presentation will examine several threats surrounding 802.11n technology, demonstrating tools that can be used to mitigate these risks.

- **Session Format *** (select one)

  ☒ Individual Speaker - You (or the designated speaker if you're submitting a proposal on behalf of someone else) will be the only speaker.

  ☐ Co-Speakers - This format has two speakers, one of whom is designated as Primary Speaker and the other as Secondary Speaker. The Primary Speaker is the person to whom the RSA Conference Speaker Manager will come with questions and decisions regarding your session.

  ☐ Panel Discussion - This is a session with a Moderator and up to four Panelists. The Moderator is responsible for facilitating the panel discussion, but is not a designated speaker. The panelists can make very short (2-3 minute) presentations to identify their individual position on the topic, but the majority of the time should be spent on Q&A. Panelists shouldn't plan to use slides. *NOTE: The positions of the individual panelists should be clarified and communicated to all the other panelists before the Conference begins.*

  NOTE: Please confirm the availability, expertise and commitment of any co-speakers and panelists before submitting their names.

- **Session Length *** 50 minutes

- **Will this presentation be seen elsewhere within 45 days before or after the Conference? ***

  No

  If Yes please specify:

- **Session Learning Objectives *** (Limit 1,000 characters including spaces)

  Evaluate the new features in IEEE 802.11n networks from a security and risk mitigation perspective
  Identify the risks associated with deploying pre-N or ratified IEEE 802.11n networks
  Apply free and inexpensive commercial tools to identify and mitigate threats introduced with 802.11n technology

- **Long Session Abstract *** (Limit 2,500 characters including spaces)

  The latest buzz in wireless LAN networking is the promise of high-speed IEEE 802.11n connectivity. This is emphasized in the consumer and commercial markets, with the availability of pre-standard "N1" and "N2" devices, as well as the recent Wi-Fi Alliance Draft-N 2.0 certification.
  While 802.11n technology represents several tangible benefits for enterprise and consumer networks, it also represents new risk areas for organizations deploying this technology, or trying to operate in a shared spectrum where other 802.11n technology is used. This presentation will examine the new features in the 802.11n and pre-N networks, and will examine several risks associated with this new technology, including availability attacks against legacy 802.11b/g networks, evading wireless intrusion detection system (WIDS) with 802.11n rogue devices, threats stemming from increase range in 802.11n networks, and attacks against new wireless drivers driven by the complexity of the 802.11n specification.
  Presenting the results of original research and analysis, the author will demonstrate live attacks stemming from the presence of off-the-shelf pre-N devices. Techniques to mitigate the risks of 802.11n networks and strategies for the secure deployment of these networks will also be covered, including the availability of tools written by the presenter and made available for free for RSA conference attendees designed to help organizations assess and mitigate these risks.

- **What pre-requisite knowledge is recommended for your audience? ***

  Understanding of the operation and use of wireless LAN environments.
  Familiarity with common wireless LAN attacks including availability and integrity attacks.

Target Audience Profiling Information –The following questions will help us accurately assess your target audience.

- **What organizational functions will be most interested in your session? *** (Select all that apply)
  ☐ Academia / Research / Scientist
  ☒ Consulting
  ☒ Engineering / Development / QA / Testing

☐ Executive
☐ Finance / Financial Analysis / Industry Analysis
☒ IT / IS / Security
☐ Legal / Operations / Procurement / Human Resources
☐ Press / Media / Public Relations / Advertising
☐ Sales / Marketing / Business Development
☐ Other

If Other please specify:

- **What job functions will be most interested in your session?** * (Select all that apply)

☐ Executive (CEO, CFO, Other CXO, President, Sr. Vice President)
☒ Executive (CTO, CIO, CSO, CISO)
☐ Vice President / Director
☒ Middle Management / Project Manager / Team Leader
☒ Front-line Employee / Regular Staff
☒ Outside Consultant
☐ Student / Academic
☐ Other

If Other please specify:

Session Profiling Information – It is obviously important to deliver a session which meets the attendee's expectations. The following information will help ensure that the attendees clearly understand what they will learn during your session.

Session Classification * Please choose one of the following:

☐ Mathematic Concepts & Principles
Advanced mathematic and cryptographic principles and theories

☐ Strategic
Designed for business oriented audiences (business line managers, directors, VPs) who are interested in business issues and strategic implications of technology. Focus should be on processes, lessons learned, tools which can be shared and results, rather than definitions and concepts.

☐ Business Futures
Designed for business professionals with 10 or more year of experience. Sessions in this category focus on new business developments, concepts, geopolitical issues or regulations that are expected to come to fruition within the next 5 years. Very little time is spent on defining terms or economic models.

☐ Advanced Technical

Sessions focused on advance technical principles and concepts, with little/no time spent on defining terms and background. Contains instructive demos, line code or advanced architecture discussions and tools that can be shared. Geared toward technical information security professionals with 10 or more years of experience.

Note: If you select this option, you will see a new field where you will need to explain why this session should be classified as "advanced technical." Please provide specific examples of what technical information you will provide.

☒ Intermediate Technical

Focused on technical principles and concepts that would appeal to information security professionals with more than 5 years of technical experience. Little, if any, time is spent on definitional terms and concepts. Contains instructive demos, line code, tools and architectural discussions.

☐ Basic Technical

Focused on technical principles and concepts that would appeal to information security professionals with less than 5 years of technical experience. Time is spent on definitions and concepts, to build up to more complex technical understanding. Job aids and tools will be a plus.

☒ Technical Futures

Designed for information security professional with 10 or more years of experience. Sessions in this category focus on new concepts, technology or threats that are expected to come to fruition within the next 5 years. Very little, if any time, is spent on defining terms; rather more time may be spent on white boarding solutions and explaining advanced theories or concepts.

☐ Advanced Legal/Compliance

Focused on practicing attorneys or corporate professionals dealing with complex intellectual property or privacy litigation or complex corporate governance, compliance and regulatory issues. These sessions assume an advanced level of legal or legislative knowledge, and are designed for practitioners with 10 or more years of experience.

☐ Intermediate Legal/Compliance

Focused on practicing attorneys or corporate professionals dealing with intellectual property or privacy litigation or corporate governance, compliance and regulatory issues. These sessions are designed for practitioners with more than 5 years of experience.

☐ Basic Legal/Compliance

Focused on practicing attorneys or corporate professionals interested in learning more about intellectual property, privacy, corporate governance, compliance and regulatory issues. These sessions assume a basic knowledge of understanding in this area, and are designed for professionals with less than 5 years of experience.

☒ Individual Contributor Professional Development

Designed for individual contributors who seek to influence others and broaden knowledge for continued career growth and/or personal goals.

☐ Manager Professional Development

Session designed for managers who seek to continue to refine management skills and business knowledge for continued career growth and/or personal goals.

☐ Advanced Professional Development

Advanced sessions for director-level and above contributors who seek to broaden their business knowledge for career growth and/or personal goals.

- **Select the track that would be most appropriate for your topic. ***

  Select that Conference Track which best fits your presentation. You will also have the opportunity to select the 2nd best fit, which will increase the odds of being selected.

  Wireless

- **What is your second choice for the track? ***

  Hackers and Threats

- **Select the security keywords which are appropriate for your session. * (Select all that apply)**
  - ☐ Access Control
  - ☐ Administrative Password Management
  - ☐ Anti-Spam
  - ☐ Anti-Virus
  - ☐ Application Security
  - ☐ Audit
  - ☐ Authentication
  - ☐ Business Continuity / Disaster Recovery
  - ☐ Certification, Security Professional
  - ☐ Compliance Management
  - ☐ Content Management/Filtering
  - ☐ Database and Storage Security
  - ☐ DDoS
  - ☐ Digital Certificates, Certificate Authorities
  - ☐ Digital Rights Management
  - ☐ Encryption and Key Management
  - ☐ End-Point Security
  - ☐ Enterprise Security Management
  - ☐ Firewalls

- ☐ Forensics
- ☐ Identity Management
- ☐ Incident Response
- ☐ Integrated Security Appliances
- ☐ Intrusion Detection
- ☐ Malicious Code Protection
- ☐ Managed Security Services
- ☐ Media Security
- ☐ Messaging Security, Email Encryption, Email Security, IM Security
- ☐ Password Management
- ☐ Patch/Configuration Management
- ☒ Penetration Testing, Vulnerability Assessment, Risk Assessment
- ☐ Physical Security
- ☐ Policy Management/Enforcement
- ☐ Product Certification
- ☐ Public Key Infrastructure (PKI)
- ☐ Remote Access
- ☐ Risk Management, Risk Analysis
- ☐ Secure e-Commerce
- ☐ Secure File Transfer
- ☐ Secure Mobile Connectivity
- ☐ Security Training, User Awareness
- ☐ Single Sign On
- ☐ Source Code Vulnerability Analysis
- ☐ Telecom/VOIP security
- ☐ Time Stamping
- ☐ VPNs
- ☒ Vulnerability Assessment
- ☐ WAN/Internet Security
- ☐ Web Content Management, Filtering/Behavior Blocking
- ☐ Web Services Security
- ☐ Web Site/Web Server Security
- ☒ Wireless Security

- **Submitters Comments**

  The speaker Joshua Wright was also a speaker at the RSA 2007 conference for the presentation "Wireless IDS Challenges and Vulnerabilities" (WIR-201).

PROPOSED SPEAKERS

Add a Speaker

An **Individual** session may have only one speaker, a **Co-Speakers** session has two speakers, and **Panel Discussions** require a moderator and up to four panelists.

All proposed speakers will be notified that they were included in a proposed submission. The Conference will proceed with the judging process assuming proposed speaker confirmation unless instructed otherwise by the proposed speakers.

Complete the following information for each speaker. You'll also be given the option to prefill the form with your information, if you are both the submitter and a speaker.

* = required input

- Session Role * Individual or Co-Speaker
- Salutation * Mr.
- First Name * Joshua
- Last Name * Wright
- Preferred Name
- Company * Aruba Networks
- Job Title * (limit 75 characters including spaces) Senior Security Researcher
- Address 1
- Address 2
- City
- State
- Postal Code
- Country
- Email address * jwright@arubanetworks.com
- Secondary email address
- Telephone * 401-524-2911
- Alternate telephone
- Fax number
- Speaker Biography/CV * (Limit 400 characters including spaces)

  Enter speaker biography/CV here

- Is the proposed speaker a Certified Information Systems Security Professional (CISSP)? *

  No

- Has the proposed speaker spoken at an RSA Conference before? *

  Yes

  If yes, please identify the Conference(s) years: 2007

- Does the proposed speaker have professional speaking experience (has he/she been paid to speak)? *

  Yes

  If yes, please elaborate where/when: Senior SANS Instructor and course author speaking at multiple SANS conferences yearly. Regular speaker at

hacker conferences including ShmooCon and DefCon.

- Will the proposed speaker be presenting at ANY event 30 days prior to the Conference? *

  Yes

  If yes, please identify the event and the title of the presentation: SANS NS2007 Conference, Assessing and Securing Wireless Networks course