

5th Annual PKI R&D Workshop: *Making PKI Easy to Use*

Program

Subject to change

Notes

802.11b Wireless access points will be available for SSH, IPSEC, HTTP, DNS, FTP, POP, IMAP, and SMTP connectivity. Only WEP access will be provide, and users must sign NIST's Visitor Network Access Agreement with regard to security patches, anti-virus software, etc.

Tuesday, April 4, 2006

8:00 am	Bus departs Gaithersburg Hilton for NIST
8:30 am - 9:00 am	Registration and Continental Breakfast
9:00 am - 9:15 am	Opening Remarks Ken Klingenstein, <i>Internet2</i> , General Chair Kent Seamons, <i>Brigham Young University</i> , Program Chair
9:15 am - 10:15 am	Keynote Address: Has Johnny Learnt To Encrypt By Now? <i>Examining the troubled relationship between a security solution and its users</i> Angela Sasse, <i>University College London</i>
10:15 am - 10:45 am	BREAK
10:45 am - 11:45 am	Session 1: Standards I Session Chair: Rich Guida, <i>Johnson & Johnson</i> How Trust Had a Hole Blown In It. The Case of X.509 Name Constraints David Chadwick, <i>University of Kent</i> Invited Talk: NIST Cryptographic Standards Status Report Bill Burr, <i>NIST</i>
11:45 am - 12:45 pm	Session 2: Standards II - Leveraging DNSSEC and PK-INIT Session Chair: Neal McBurnett, <i>Internet2</i> Invited Talk - Trust Infrastructure and DNSSEC Deployment Allison Mankin, <i>Consultant</i> Invited Talk - Integrating Public Key and Kerberos Jeffrey Altman, <i>Secure Endpoints Inc.</i>
1:00 pm - 2:00 pm	LUNCH

Please note: There will not be bus service back to the hotel on the afternoon of Thursday, April 6.

2:00 pm - 3:30 pm	<p>Session 3: Revocation Session Chair: Von Welch, <i>NCSA – University of Illinois</i></p> <p>Invited Talk – Enabling Revocation for Billions of Consumers Kelvin Yiu, <i>Microsoft</i></p> <p>Navigating Revocation through Eternal Loops and Land Mines Santosh Chokhani & Carl Wallace, <i>Orion Security Solutions, Inc.</i></p>
3:30 pm – 4:00 pm	BREAK
4:00 pm - 5:30 pm	<p>Session 4: Easy-to-Use Deployment Architectures Session Chair: Stephen Whitlock, <i>Boeing</i></p> <p>Simplifying Credential Management through PAM and Online Certificate Authorities Stephen Chan & Matthew Andrews; NERSC / Lawrence Berkeley National Lab</p> <p>Identity Federation and Attribute-based Authorization through the Globus Toolkit, Shibboleth, GridShib, and MyProxy Tom Barton, University of Chicago Jim Basney, NCSA/Univ of Illinois Tim Freeman, University of Chicago Tom Scavo, NCSA/University of Illinois Frank Siebenlist, MCSD, Argonne National Laboratory Von Welch, NCSA/University of Illinois Rachana Ananthakrishnan MCSD/ Argonne National Lab Bill Baker, NCSA/University of Illinois Monte Goode, Lawrence Berkeley National Laboratory Kate Keahey, MCSD/Argonne National Lab</p> <p>PKI Interoperability by an Independent, Trusted Validation Authority Jon Ølnes, DNV Research; Norway</p>
5:30 pm	Bus Departs for Gaithersburg Hilton
6:00 pm	Dinner Buffet – Gaithersburg Hilton

Please note: There will not be bus service back to the hotel on the afternoon of Thursday, April 6.

Wednesday, April 5, 2006

8:15 am **Bus departs Gaithersburg Hilton for NIST**

8:30 am - 9:00 am **Registration and Continental Breakfast**

9:00 am - 10:30 am **Session 5: Panel - Digital Signatures**
Panel Moderator: David Chadwick, *University of Kent*

Panel members

Ron DiNapoli, *Cornell University*
Anders Rundgren, *RSA Security*
Ravi Sandhu, *George Mason University*

10:30 am - 11:00 am **BREAK**

11:00 am - 12:45 pm **Session 6: Domain Keys Identified Mail (DKIM) and PKI**
Session Chair: Barry Leiba, *IBM*

Achieving Email Security Usability

Phillip Hallam-Baker, *VeriSign, Inc.*

DKIM Panel Members

Jim Fenton, *Cisco*
Phillip Hallam-Baker, *VeriSign, Inc.*
Tim Polk, *NIST & IETF PKIX Co-chair*

1:00 pm - 2:00 pm **LUNCH**

2:00 pm - 3:30 pm **Session 7: Work in Progress (WIP)**
Session Chair: Krishna Sankar, *Cisco Systems*
Impromptu Rump Session (Sign-ups will be taken prior to the WIP by Jason Holt)

Scheduled topics:

- Experiences Securing DNS through the Handle System
 - Sam Sun, *CNRI*
- International Grid Trust Federation: How to Build Trust Across the Global Grid
 - Michael Helm, *ESnet Berkeley Lab*
 - Doug Olson, *Lawrence Berkeley Nat'l Lab*
- Suite B Enablement in TLS: A Report on Interoperability Testing Between Sun, RedHat, and Microsoft
 - Vipul Gupta, *Sun*
 - Robert Relyea, *RedHat*
 - Kelvin Yiu, *Microsoft*

3:30 pm - 4:00 pm **BREAK**

Please note: There will not be bus service back to the hotel on the afternoon of Thursday, April 6.

4:00 pm - 5:30 pm

Session 8: Panel - Browser Security User Interfaces
Why are web security decisions hard and what can we do about it?

Panel Moderator: Jason Holt, *Brigham Young University*

Panel members

Amir Herzberg, *Bar Ilan University*

Sean Smith, *Dartmouth University*

George Staikos, *KDE*

Kelvin Yiu, *Microsoft*

5:30 pm

Bus Departs for Gaithersburg Hilton

Please note: There will not be bus service back to the hotel on the afternoon of Thursday, April 6.

March 29, 2006

Thursday, April 6, 2006

- 8:15 am **Bus departs Gaithersburg Hilton for NIST**
- 8:30 am - 9:00 am **Registration and Continental Breakfast**
- 9:00 am - 9:30 am **Session 9: PKI in Higher Education**
Session Chair: Eric Norman, *University of Wisconsin*
- CAUDIT PKI Federation - A Higher Education Sector Wide Approach**
Viviani Paz, *Australian Computer Emergency Response Team*
Rodney McDuff, *The University of Queensland*
- 9:30 am - 10:45 am **Session 10: Panel - Federal PKI Update**
Panel Moderator - Peter Alterman, *National Institutes of Health*
- Panelists**
Judy Spencer, *General Services Administration*
David Cooper, *NIST*
- 10:45 am – 11:15 am **BREAK**
- 11:15 am - 12:30 pm **Session 11: Panel - Bridge to Bridge Interoperations**
Panel Moderator - Peter Alterman, *National Institutes of Health*
- Panelists**
Debb Blanchard, *Cybertrust*
Santosh Chokhani, *Orion Security Systems, Inc.*
Scott Rea, *Dartmouth College*
- 12:30 pm - 12:45 pm **Wrap up**

Please note: There will not be bus service back to the hotel on the afternoon of Thursday, April 6.