



### NEWSLETTER INFORMATION

Published nine times per year (September – June) by the Minnesota Information Professional Society. We welcome materials for publication (articles or news). Submit materials on disk or via E-mail to:

Earl C Joseph  
365 Summit Avenue  
St. Paul, MN 55102  
Tel. (651) 290-2846  
E-mail: ejoseph@waldenu.edu

### NOTE MEETING INFORMATION

**MEETING PLACE:**  
**Holiday Inn – Bloomington**  
**35W at 94<sup>th</sup>**  
**Phone (612) 884-8211**

**Meeting Times:**  
5:00 PM Social Hour  
6:00 PM Dinner  
6:45 PM Meeting & Program  
8:00 PM Adjourn

For Reservation Call:  
John Belich  
by January 11<sup>th</sup> and choose:  
Roast Beef or  
Chicken Supreme  
  
Tel: (651) 634-1440  
or e-E-mail:  
[john.belich@tech-pro.com](mailto:john.belich@tech-pro.com)

\$20 Members  
\$25 for non-members

### Dinner Meeting NOTICE

Tuesday  
January 15, 2002

Meeting of

**Minnesota Information  
Professional Society**

Speakers Topic:  
**“E-COMMERCE GONE  
BAD: WHAT TO DO  
WHEN YOU GET BIT”**

Speaker:  
**Arnold W. Kwong**

The age of the great Internet E-Commerce roll-out is past. Executive management and sales groups no longer give developers "blank checks" in pursuit of 'the ultimate web experience' to convince customers and business partners to cozy up. Management and other players now expect that web sites will pay their own way by advertising returns and market value, or by cost savings processing interactions with business partners. Even with the benefit of hindsight over the past Internet boom period and evermore sophisticated 'cool tools' to help, big questions remain for webmasters and IT management.

This session is about those web sites that were "not as successful as planned." As technology professionals what do we say and do when our own organization's web site, or that

of a friend, "doesn't work"? Is there a conspiracy in embarrassed silence? What is to be done? Where do you restart when the e-commerce site doesn't?

The session will start with a brief overview of the types of failures and likely causes, and then move on to the action plans that can be proposed to keep sites moving forward. Particular attention is paid to those processes and technology elements that are understood to cost more, deliver less, and that cause the most lost sleep.

The session will be focused to the pragmatic efforts:

- 1) What must be done?
- 2) How can costs to both maintain and enhance the web site be controlled?
- 3) How are the conditions that can cause continuing failures or losses be avoided?

Bring your questions and war stories for discussion and debate!

### Speaker Profile

Arnold W. Kwong is a former TCACM Chapter Chair who now works with both technical and management issues at Extratelligence. He brings more than 20 years of experience, including a stint at the Gartner Group, to distill the realities of organizational life

down to getting the technical work done.

## **President's Letter**

Happy New Year to you and your family & friends! I hope that you had an enjoyable holiday season. MnIPS is starting up its monthly meetings again after its December recess. The January-May meetings will continue to be held on the third Tuesday (January 15, February 19, March 19, April 16 and May 21).

MnIPS is a volunteer organization and we always welcome any help in our regular, ongoing committees or at a specific event, such as registering people at monthly dinner meetings (during 5-6pm) or at the Golf Outing in June. A new member that recently stepped forward to help is Sylvia Wiebe. Sylvia is our new Webmaster (i.e., the [www.mnips.org](http://www.mnips.org) website maintenance person). Thanks for your help, Sylvia!

We also welcome ideas from you that can improve our organization. If you can assist us this year in any capacity please let me or any board members (that are listed on the back page) know.

I would like to welcome the newest MnIPS members that have joined our group the past year. The current and established MnIPS members have found their participation in MnIPS (and ASM/ACM in the past) a rewarding experience. We will mail out membership renewal forms to the veteran membership this month. Those who have attended MnIPS meetings regularly in the past few years will also receive a membership invitation in the mail during January. I hope that each of

you consider joining MnIPS for 2002.

I look forward to hearing our January 15<sup>th</sup> meeting's speaker, Arnold Kwong of Extratelligence, who will speak on "E-Commerce Gone Bad: What To Do When You Get Bit". Our February and March speakers will be Bruce Heaton and Anita Cassidy (Planning for E-Business success), respectively.

Thanks to our November 21<sup>st</sup> presenter, Bob Burkhart, who talked about "Cyber-Terrorism". Thanks also to our October 16<sup>th</sup> speaker, Todd Hudspeth of Espiria Consulting, who spoke on "E-commerce and Intrusion Detection". For a summary of Todd's talk, please read the regular meeting review column in this newsletter.

I hope to see all of you at the January 15 meeting!

--Dennis Cummings, MnIPS President

### **Eliminate Confusion over System Intrusion!**

(October 2001 MnIPS meeting review, written by Dennis Cummings)

Mr. Todd Hudspeth was the featured presenter on "E-commerce and Intrusion Detection" at the Minnesota Information Professional Society's monthly dinner meeting held on October 16, 2001 at the Bloomington Holiday Inn. He is the Principal Security Architect and CISSP for Espiria, a national consulting firm specializing in total security solutions. He has designed, architected, and engineered multi-firewall environments for multiple

Fortune 500 corporations. Prior to moving to the Twin Cities, Mr. Hudspeth was the Manager of Corporate Systems Security for Turner Broadcasting System, Inc. in Atlanta, where he was responsible for the development and implementation of the Turner corporate systems security policies and procedures and corporate firewall architecture.

Mr. Hudspeth asked the MnIPS crowd "Are you sure your system isn't being quietly subverted at this moment by a Hacker?" He provided an in depth look at intrusion detection, including proactive monitoring and response processes. This presentation examined the types of Intrusion Detection Systems (IDS's), the pros and cons of using them, the risks involved, the support considerations and ways an IDS can be defeated. This presentation also acknowledged that IDS is not the be-all end-all in security, but rather, one critical component in a layered security model – and a very intelligent way to know what is going on in your environment.

Mr. Hudspeth's objectives were to introduce the attendees to: Intrusion Detection Systems (IDS's), types of IDS's, their Pros & Cons, their risks, their support considerations, different ways to defeat IDS's and what further resources are available to study "system intrusion". He defined IDS's as systems that apply the art of detecting inappropriate, incorrect or anomalous activity. They can be found in network, host and hybrid systems. In comparison to physical security, IDS is the burglar/theft alarm for the network and systems.

Network IDS's use "network cards" in promiscuous mode, sniffing all packets on each network segment. They also consist of sensors and management console to analyze and aggregate data from sensors. Host IDS's look only at packets addressed to the computer on which it resides and/or watches processes inside the host. They may be entirely independent, or report to a master system. Hybrid IDS's combine a host IDS with a network IDS. Their implementation depends upon each product, which can be difficult to define.

Mr. Hudspeth identified 2 classes of system intrusions. They are "misuse" and "anomaly" intrusions. "Misuse" intrusions are attacks on known weak points of a system, and it compares network traffic with signatures of known attacks. "Anomaly" intrusions are unknown attacks and other anomalous activity that requires intimate knowledge of the specific network and patterns of user behavior. It may include detection of an intruder who is already inside a network.

Mr. Hudspeth then presented the positive and negative aspects of IDS's as well as their risks. IDS's positive features are that they can provide: real-time monitoring and alarming, a proactive approach to detecting intrusions, assistance in investigating data and as a complement to an overall security architecture. IDS's negative features are that they can: be very difficult or complex to implement, filter false alarms, require additional support staff time, be constantly changing, require constant care and feeding,

provide a false sense of security, and be problematic trying to detect unknown threats to the system.

IDS's risks are that: they are not a panacea and cannot do the job alone, they are not a substitute for good security policy and planning, its technology is still relatively new, and strong identification and authentication to the system may be still required.

Installing an IDS does require several support considerations such as:

1. Extensive vendor and security training for support personnel.
2. Defined security policies and procedures.
3. Incident response procedures.
4. Incident response team.
5. Enhanced security training.
6. IT forensics.
7. Secure network and system architecture.
8. Trained and active monitoring/review staff.
9. Appropriate log storage capabilities.
10. System and network device hardening procedures.
11. Strong vendor support.
12. Combination of security tools/devices.
13. Monitor incoming and outgoing traffic.
14. Choose the best product for your environment and use only what can be supported.
15. Constant monitoring for new attack signatures.
16. Sound and enforced change management policy.
17. Authorization process.
18. System testing environment.
19. Consider outsourcing alternatives.

However, the support staff should be aware of the many ways to overcome IDS's like:

1. Incomplete IDS coverage.
2. Lost or unknown network elements.
3. An overwhelmed IDS.
4. Excessive false positives.
5. Fragmented packets.
6. The 0-day problem.
7. Highly switched networks.
8. Compromise of the IDS itself.
9. Improperly configured IDS.

Finally, Mr. Hudspeth offered several websites where the attendees can learn more about IDS's and they are listed below. If you wish to learn more about Mr. Hudspeth or his Espiria work, please contact him by email at "[thudspeth@espiria.com](mailto:thudspeth@espiria.com)".

1. [http://www.messageq.com/security/meinel\\_3.html](http://www.messageq.com/security/meinel_3.html)
2. <http://www.robertgraham.com/mirror/Ptacek-Newsham-Evasion-98.html>
3. <http://www.securityfocus.com/focus/ids/articles/idsterms.html>
4. [http://www.sans.org/infosec/FAQ/intrusion/intrusion\\_list.htm](http://www.sans.org/infosec/FAQ/intrusion/intrusion_list.htm)
5. <http://secinf.net/iidse.html>
6. <http://www.scmagazine.com/index2.html> (this site includes a July/2001 IDS product comparison)
7. <http://www.cerias.purdue.edu/coast/intrusion-detection/welcome.html>
8. <http://www.cerias.purdue.edu/coast/ids>.

## MnIPS Officers 2002

President  
Dennis Cummings (W) 651-205-2632

Vice President  
Gerry Lindner (W) 651-292-9304

Past President & Treasurer  
Joe Perzel (W) 612-340-1110

Programs  
Kurt Linberg (W) 612-252-4335

Marketing  
Joe Reilly (W) 612-513-5951

Secretary  
Bob Burkhart (W) 952-888-1108

Arrangements  
John Belich (W) 651-634-1440

Newsletter Editor  
Earl C. Joseph (W) 651-290-2846

Education  
Hazel Matias (W) 612-627-2171

Summer Golf Outing  
Jeff Hemauer (W) 651-766-1387

Audit & Bylaws  
Dave Farmer (W) 651-637-2568

Special Projects  
Bill McTeer (W) 612-333-4115

Data Base  
Tom Walters (W) 952-995-4066

**MnIPS Newsletter**  
P.O. Box 201243  
Bloomington, MN 55420-1243

### Address Service Requested

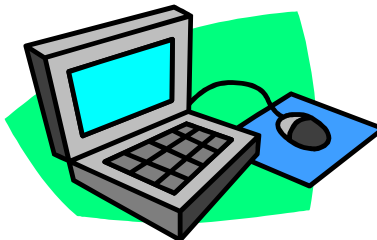
#### **DINNER MEETING**

Tuesday, January 15, 2002 – 5-8PM  
TOPIC

“E-COMMERCE GONE BAD: WHAT TO  
DO WHEN YOU GET BIT”

**NOTE: Meeting Location**  
Holiday Inn Bloomington  
35W & 94<sup>th</sup> (1201 W. 94<sup>th</sup> St.)

**“IN 50 YEARS THE  
TYPICAL COMPUTER  
HAS BECOME 10,000  
TIMES LESS COSTLY,  
10,000 TIMES FASTER,  
AND WEIGH 10,000  
TIMES LESS!”**



by Earl C. Joseph