

Email Security

**Presented to the Puget Sound Chapter
Information Systems Audit & Control
Association**


**September 18, 2003
Sandy Bacik, CISSP, CISM
Engagement Manager
Technology Solutions Services
Jefferson Wells International**



Agenda


- **What is e-mail and is it really like a postcard?**
- **Corporate policy & email liabilities**
- **Secure e-mail?**
- **Tools and techniques**
- **Tech Session - Reading email headers**

©Sandra Bacik



Let's take a test


©Sandra Bacik



What is NOT true about email?

- A) Email stands for electronic mail
- B) You can attach documents using email
- C) Email is difficult to use
- D) Email allows you to quickly contact someone on the other side of the world


©Sandra Bacik



email address san04@att.edu.au, the att.edu.au part of the address tells you

- A) san04 has an account on the server called att**
- B) san04 got an account through an educational institute**
- C) san04 has an Australian email account**
- D) All of the above**

©Sandra Bacik



You can email somebody even if you don't know their email address

- A) True**
- B) False**

©Sandra Bacik



**You can tell where a person is from
when you look at their email address?**

- A) True**
- B) False**
- C) In some cases, but in
others you can't**

©Sandra Bacik



Email Pros

- Fast and easy for business**
- Personal tone**
- Inexpensive**
- Easy responses, forward, reply**
- Good for project collaborations**
- Reach many people**

©Sandra Bacik



Email cons

- **Questionable appropriateness**
- **Formatting may be lost**
- **Not necessarily secure and confidential**
- **Can accidentally be forwarded**
- **No original hard copy with signature**

©Sandra Bacik



Issues Related to Email

- **Viruses**
- **Spam**
- **Business use**
- **Retention**
- **Privacy**


©Sandra Bacik



Email Advantages

- **Keep in touch with others**
- **Short send time and no interruption at other end**
- **Share ideas and promote opinions**
- **Join discussion groups**
- **Attach fun things**


©Sandra Bacik



Email Limitations

- **Not private**
- **Some are only text based**
- **Easy to forge email**
- **Easy to intercept**


©Sandra Bacik



Email States

- **Stored on the server**
- **Stored on the client**
- **Transit**
- **Printed**


©Sandra Bacik



The Journey of an Email

- **Emails are addressed and sent to one another based on a naming and routing system the Internet understands.**
- **Just as the United States Postal Service has a system for identifying people at particular locations, so does the Internet for email.**

©Sandra Bacik




The Journey of an Email

- **Components of a U.S. mailing address**
 - One identifies a particular person.
 - The other identifies the location of that person in the United States.

John Doe
123 Somewhere Rd
Sacramento, CA 95831

©Sandra Bacik

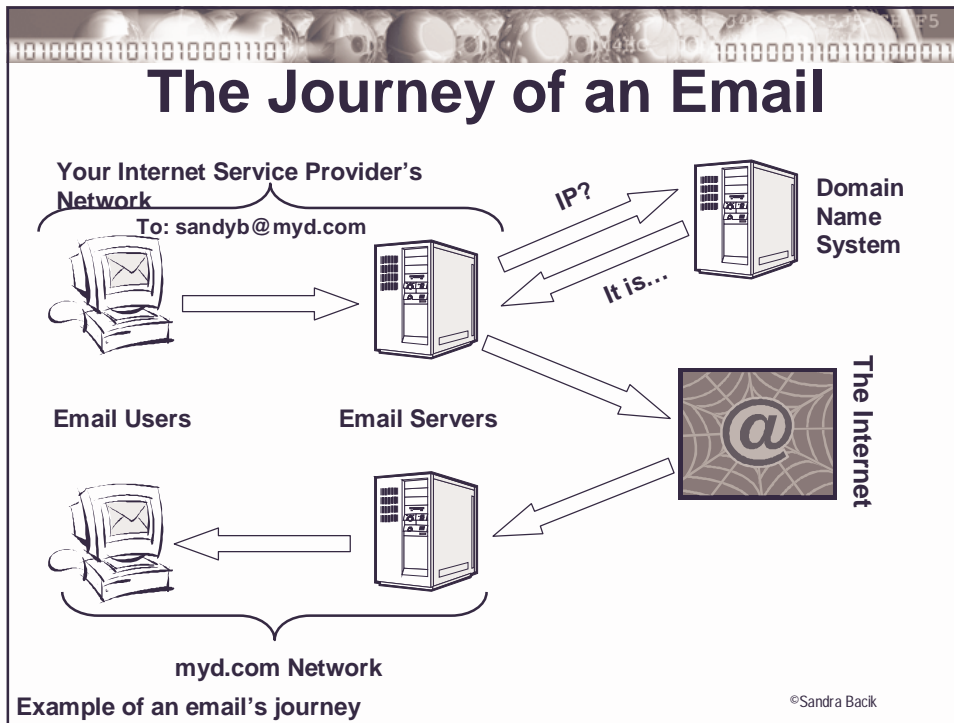


The Journey of an Email

1 2 3
san04@worldnet.att.net


- 1 Local address
- 2 Server handling email
- 3 Internet domain name

©Sandra Bacik




Liabilities and issues with email and corporate policy

©Sandra Bacik



Email can create a large corporate liability. Email established a permanent written record of internal, and some external, communications that may have only been oral in the past.

©Sandra Bacik



What are email weak links?

- **Employees**
- **Network infrastructure**
- **Policies**
- **Remote use**

©Sandra Bacik



Email gossips put employers at risk. Gossiping or slating colleagues behind their backs might be a common, if unfortunate, workplace occurrence but doing it on email could have serious repercussions, as one employer found out last week. A woman who discovered nine of her colleagues had circulated offensive emails about her has received £10,000 compensation after settling a sexual harassment case against her former employer. <http://www.theregister.co.uk/content/67/32489.html>

©Sandra Bacik



Email related threats (1)

- **Privacy**
- **Spam**
- **Information leaks - intellectual property**
- **Embarrassments, harassment and threats**

©Sandra Bacik



Email related threats (2)

- **Viruses**
- **Delivery failure or mis-delivery**
- **Denial of service**
- **Interception and tampering**
- **Redirection**
- **Impersonation**

©Sandra Bacik



Spam

Unsolicited commercial e-mail

©Sandra Bacik

2003/01 - Study: Spam cost U.S. corporations \$8.9 billion. All those junk e-mail messages may promise instant wealth, but they can be quite painful to the bottom line. A study to be released attempts to quantify the annual cost of spam: \$8.9 billion for U.S. corporations, \$2.5 billion for European businesses and another \$500 million for U.S. and European service providers.

<http://www.cnn.com/2003/TECH/biztech/01/03/spam.costs.ap/index.html>

Net users want law to can spam


<http://zdnet.com.com/2100-1106-979108.html>

©Sandra Bacik

Cost of Spam

- **Server hardware to store messages**
- **Bandwidth**
- **Upgraded clients to handle storage and processing of extra software**
- **Connection fees**
- **Loss of productivity**

©Sandra Bacik



Solutions

- **Get rid of corporate email**
- **Filtering software (content, header, site)**
- **Third party open relay block list**
- **Blocking internal addresses from the Internet**
- **User education**

©Sandra Bacik



Secure email

Guarantee the message arrives to the intended recipient while retaining confidentiality.

©Sandra Bacik



Protecting the network

- Security policy
- Security software
- Encryption
- Content control
- Virus scanning

©Sandra Bacik



Email policy

- Who owns the content
- Business use only
- Right to monitor and inspect
- A user accepting an account constitutes agreement with policy
- Training

©Sandra Bacik

Define Restrictions

- **Unauthorized attempts to access another's email is a policy violation**
- **Sensitive or proprietary information transmission is prohibited outside the company**

©Sandra Bacik

Where to Put Policy

- **Signature acknowledgment upon hire**
- **Regular signature renewal**
- **Employee handbook**
- **Email notices**

©Sandra Bacik



Monitoring

- **Monitoring contents is restricted by law, but monitoring headers is not**
- **Electronic Communications Privacy Act of 1986**
- **Specific state laws**
- **“public” versus “private” email**

©Sandra Bacik



Records Retention

- **Online storage limits - size and date**
- **Backup requirements**
- **Destruction of data**

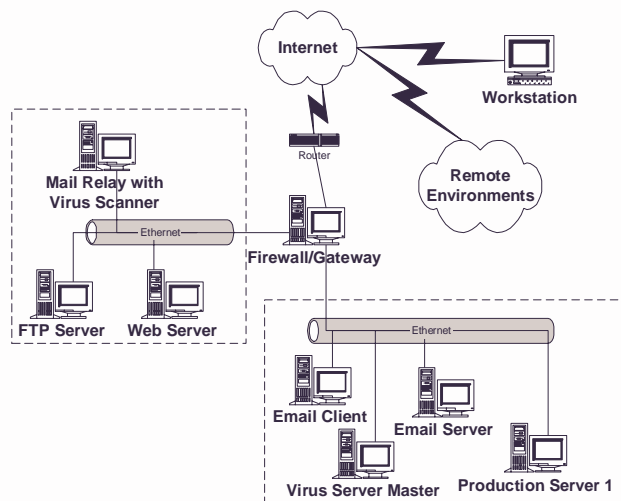
©Sandra Bacik

Types of protection

- Email footers
- Encryption
- Digital signatures
- Content filters
- Email tracking
- Anti-virus

©Sandra Bacik

Layered Network Protection



©Sandra Bacik



How to minimize the human factor

- **Standardized email package**
- **Standardized email client**
- **Standardized virus package**
- **Keeping current with patches and/or service packs**

©Sandra Bacik



Tools & Techniques

©Sandra Bacik

Email Protocols

- **SMTP – Simple Mail Transport Protocol (port 25)**
- **POP – Post Office Protocol (ports 109, 110, 995)**
- **IMAP – Internet Message Address Protocol (ports 143, 220, 585, 993)**

©Sandra Bacik

Standard External Footer

NOTICE: This communication may contain privileged, limited, sensitive or other confidential information. If you are not the intended recipient, or believe that you have received this communication in error, please do not print, copy, retransmit, disseminate, or otherwise use this information in-whole or in-part. Please notify the Sender that you received this e-mail in error, and delete the copy you received.

©Sandra Bacik



Securing the Mail Server (1)

- **Rejecting messages not destined for internal addresses**
- **Block mail relaying**
- **Change SMTP banner**
- **Review email aliases**

©Sandra Bacik



Securing the Mail Server (2)

- **Limit number of SMTP inbound connections from the same IP**
- **Review to ensure your server has not been blacklisted**
- **Regular monitoring**

©Sandra Bacik

SMTP Commands


- HELO
- MAIL FROM
- RCPT TO
- DATA
- QUIT

©Sandra Bacik

How to get someone's email

- Company directory
- Return address
- Web-based “white pages”
- Directories for collections or lists of addresses


©Sandra Bacik



Pieces of an email

- **Header**
- **Message body**
- **Signature**
- **Attachments**

©Sandra Bacik



Getting around email systems

- **Some servers remove header information**
- **Faking it/Spoofing - from line**
- **Remailers**
- **Relaying**
- **Stealing accounts**

©Sandra Bacik



Why use encryption?

- Confidentiality of content
- Verify receipt and sender
- Secure file transfers using SMTP as the transport
- Secure inter- and intra-company communications

©Sandra Bacik



Succeeding with Secure Email

- If it's not easy/simple/transparent it's not going to get used
- Need the ability to centrally manage
- Support across many email systems
- Content and virus scanning

©Sandra Bacik



Some Popular Methods

- Password based
- PKI - S/MIME
- PKI – PGP
- Web based solutions
- Key server solution

©Sandra Bacik



Tracking email

- Email client
- Email server
- Firewall or proxy logs
- Browser
- Steganography

©Sandra Bacik



Quick Tips

- **Don't click executable attachments**
- **Beware e-mails from people you do/don't know**
- **Install security updates**
- **Scan incoming e-mail for viruses**
- **Harden your e-mail client**
- **Don't respond to Spam e-mail**

©Sandra Bacik



Summary


- **How liable is your company?**
- **Securing email**
- **Corporate policy**
- **Where to go for help**

©Sandra Bacik



Contact Information:
Sandy Bacik, CISSP, CISM
Engagement Manager
Technology Solutions Services
Jefferson Wells International
701 Fifth Avenue, Suite 2840
Office: 206-664-2738
email: Sandra_Bacik@jeffersonwells.com

©Sandra Bacik



**Tech Session – Reading
email Headers**

©Sandra Bacik



Explanation of Headers

Takes you through a normal header, email through firewalls, and mail relaying headers.

<http://www.stopspam.org/email/headers/headers.html>

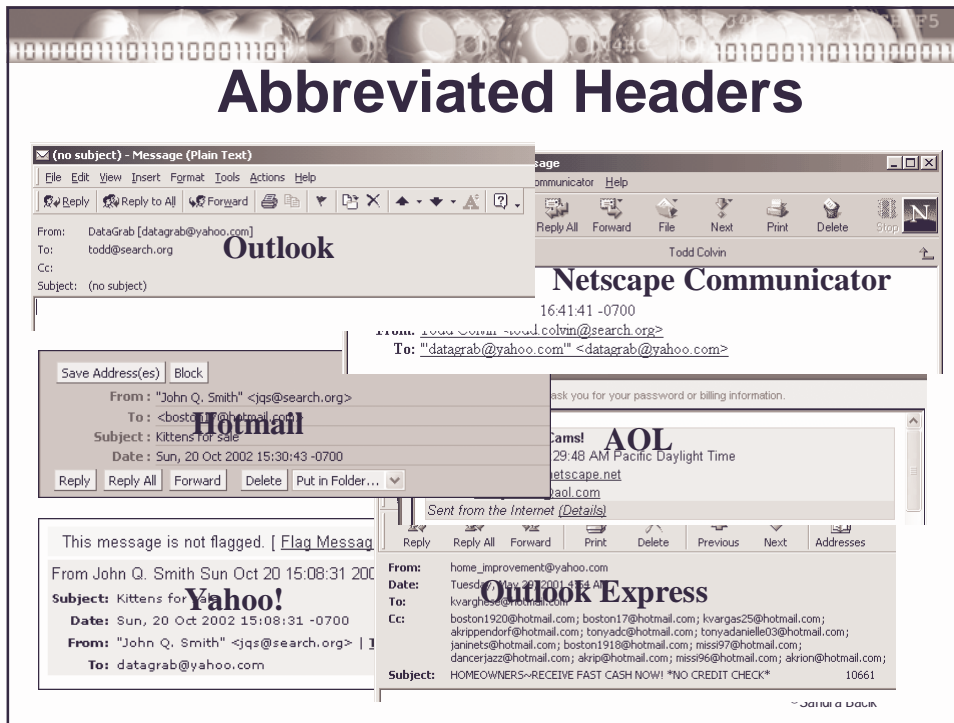
©Sandra Bacik



Email Tracing

- **To determine the sender of an email, an investigator needs the email's header information.**
- **An email header is the information added to the beginning/top of the electronic message.**
- **By default, email clients and services only show an abbreviated form of the header.**

©Sandra Bacik



Email Tracing – Short Header

- Information displayed in the abbreviated view are the memo header items:
From To CC Subject Date
- This is not enough information to properly trace an email.

Email Tracing – Complete Header

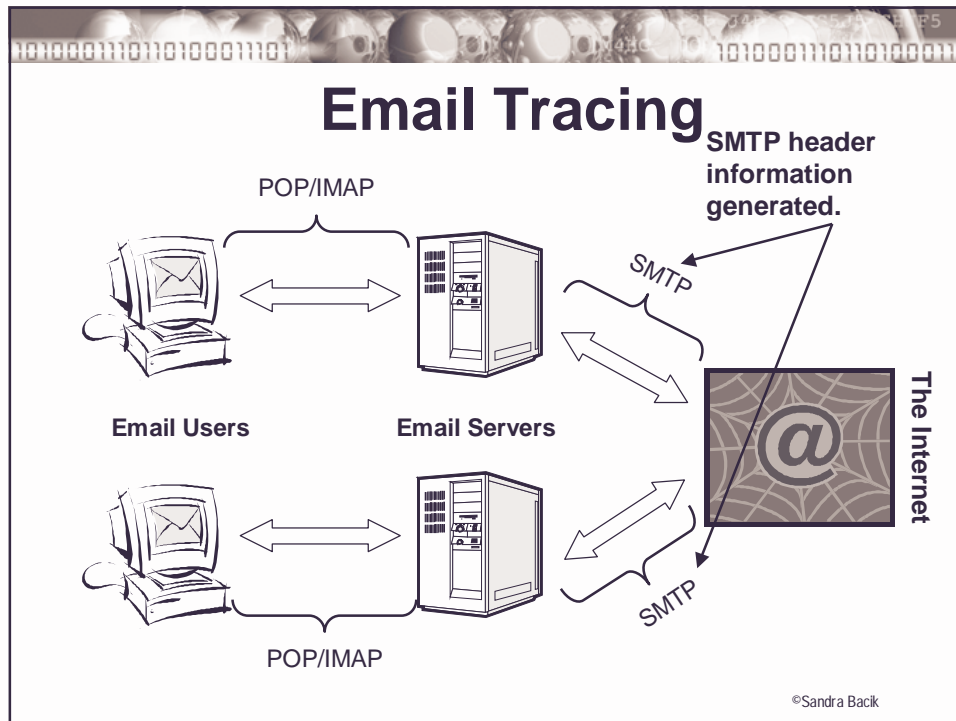
- Who sent the email.
- Which network it originated from.
- Which email servers processed it.
- Miscellaneous information:
Timestamps, Email client, Encoding information, etc.
- Some of it is useful for tracing email, some of it is not.

©Sandra Bacik

Email Tracing

- Headers are created by the email servers that process messages for delivery.
- Not every server adds detailed information to the header, depends on the email protocol used.
- Headers of the type seen in the previous example are created by servers using the SMTP to transfer email to its destination.

©Sandra Bacik



Email Header Details

- **RFC 2076 – Common Message Headers**
 - ♦ A table of commonly occurring header fields and a short description of what they mean and what their status is (e.g., standard or not).
 - ♦ Not exhaustive.
 - ♦ <http://www.ietf.org/rfc/rfc2076.txt>

©Sandra Bacik

Email Header Details

- **No limits on the number of fields. Senders can create fields.**
- **Only two types are required. Origination date field “Date:” and at least one of the originator fields:**
 - **From:**
 - **Sender:**
 - **Reply-To:**

©Sandra Bacik

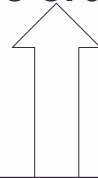
Email Header Details

- **Header fields of particular interest:**
 - ♦ **The originator fields -**
 - **From:, Sender:, Reply-To:**
 - ♦ **Date:**
 - ♦ **Received:**
 - ♦ **X-Originating-IP:**
 - ♦ **Message-ID:**
 - ♦ **X-Mailer:**
 - ♦ **X-MIMEOLE:**

©Sandra Bacik

Email Tracing – Header Structure

- The fields are loosely organized in a layered, bottom-to-top sequence.
 - ◆ Few limitations on the order. Mostly apply to certain fields (e.g., Received and Return-Path).
- First field is on the bottom, subsequent fields added on top, in the order they are written.



©Sandra Bacik

Email Tracing

- How many email servers a message will pass through depends on the networks it passes through.

- Then the third email server adds information and so on until the destination is reached.

- The second email server adds information next.

- The first email server to receive the message via SMTP is the first to add information into the header.

3...

2

1

©Sandra Bacik

Tracing an Email

- Finding the sender's email address
- Finding the originating IP address with the server logs
 - ♦ The IP address of the system used by the email sender.
 - ♦ The sender's user ID.
 - ♦ The host name of the sender's computer.
 - ♦ The Message-ID assigned to the email sent by the sender.

©Sandra Bacik

Potential Problems

- All fields in an email header can be forged by the sender except for the fields added by servers not under the sender's control. Forgeable fields include:
 - ♦ From:, Bogus, additional "Received" fields not created by actual servers, X-Originating-IP:, Message-ID:, Reply-To:

©Sandra Bacik

IP Address Tracing Goals

- **Determine to whom the IP address is assigned.**
 - ◊ **Usually a business of some sort.**
 - ◊ **Often an Internet Service Provider (ISP) in the case of email.**
- **Contact the entity it is assigned to.**
 - ◊ **From their records, determine the identity of the person using that address at the date and time in question.**

©Sandra Bacik

IP Address Tracing

- **IP addresses are allocated to organizations and people by Regional Internet Registries (RIRs).**
- **Currently, there are 3 RIRs responsible for the administration and registration of IP addresses for the entire global Internet.**
 - ◊ **Each RIR performs this task for different geographical areas.**
 - ◊ **There may soon be 2 new RIRs.**

©Sandra Bacik



IP Address Tracing

- **Asia Pacific Network Information Centre (APNIC)**
 - ◊ **Responsible for the Asia Pacific region.**
 - **Asia and Oceania**
 - **62 Countries**
 - ◊ **<http://www.apnic.net>**

©Sandra Bacik



IP Address Tracing

- **American Registry for Internet Numbers (ARIN)**
 - ◊ **Responsible for North America, South America, Caribbean, and Sub-Saharan Africa.**
 - **70 Countries**
 - ◊ **<http://www.arin.net>**

©Sandra Bacik

IP Address Tracing

- **RIPE Network Coordination Centre (RIPE NCC)**
 - ♦ **Responsible for Europe, The Middle East, the North of Africa, and parts of Asia.**
 - **107 Countries**
 - ♦ **<http://www.ripe.net>**

©Sandra Bacik

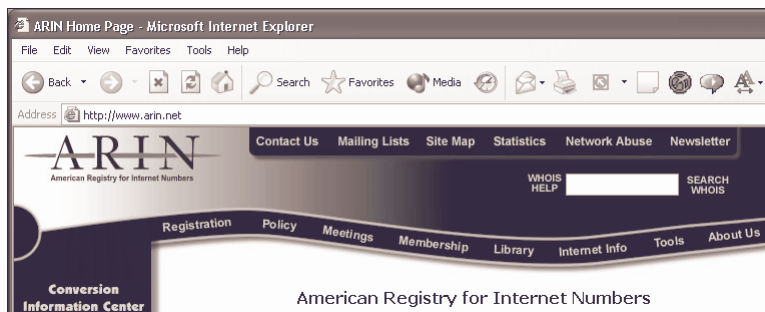
IP Address Tracing – Emerging RIRs

- **Latin American and Caribbean IP address Regional Registry (LACNIC)**
 - ♦ **Will be responsible for Latin American and Caribbean Region.**
 - ♦ **<http://lacnic.net>**
- **African Network Information Center (Afrinic)**
 - ♦ **Will be responsible for continent of Africa.**
 - ♦ **<http://www.afrinic.org>**

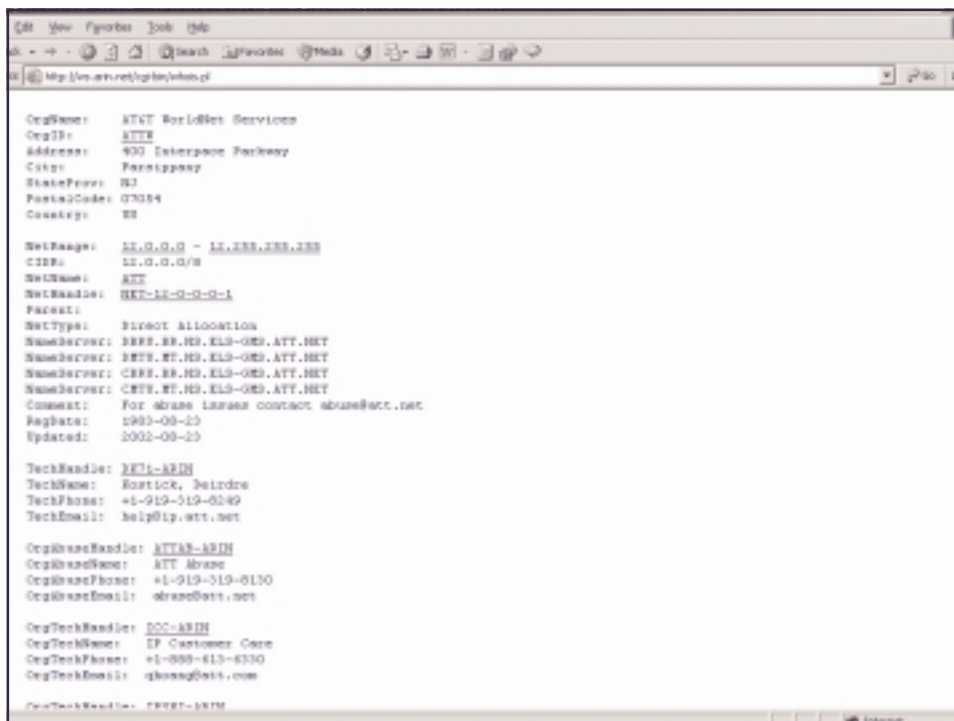
©Sandra Bacik

Find the Originating IP Address

- To determine which organization is responsible for the administration of the originating IP address, use the WHOIS service of one of the Regional Internet Registries.



©Sandra Back





Contact Information:
Sandy Bacik, CISSP, CISM
Engagement Manager
Technology Solutions Services
Jefferson Wells International
701 Fifth Avenue, Suite 2840
Office: 206-664-2738
email: Sandra_Bacik@jeffersonwells.com

©Sandra Bacik