



PRESS RELEASE

FOR IMMEDIATE RELEASE

CONTACT: LIZ LANDIS
IRONPORT SYSTEMS
415.828.4801 MOBILE
LLANDIS@IRONPORT.COM

IronPort Systems Reports Results of Email Authentication Efficacy Study

Groundbreaking Study of Enterprise and ISP Traffic Shows That Reputation Data Is Essential to Improving Authentication Results

SAN BRUNO, Calif. and NEW YORK, NY, — July 12, 2005 – IronPort Systems, the market share leader in email security, today announced the results of a study on email authentication efficacy at the Email Authentication Summit being held at the Marriot Marquis in New York City. Leveraging IronPort's SenderBase™ Email Traffic Monitoring Network, the study goes beyond Sender ID Framework (SIDF) adoption statistics to present data on authentication efficacy and demonstrate the use of reputation data to boost efficacy tenfold. To maximize the positive impact of authentication, there must be a real-world understanding of the issues and technology limitations. The IronPort Email Authentication Study was architected to understand what's working, what's not working and why.

"Results from the IronPort study conclude that adding reputation data to email authentication significantly increases efficacy," said Patrick Peterson, Vice President of Technology for IronPort Systems. "The Email Authentication Summit is a perfect forum to discuss how to integrate this critical component. IronPort is pleased to be participating in the Summit and we are honored to be in a position to provide the valuable reputation data that's needed for authentication technology to deliver its full promise."

60% of All Email with Sender ID Framework Fails Authentication

The IronPort Email Authentication Study reveals that over 50% of all email with Sender ID Framework records fails authentication; and only half of these authentication failure messages are highly likely to be spam. The study shows 3% of all registered domains are now publishing records. However, these represent 14% of all domains actively sending email and account for a third of all Internet email sent. The most surprising finding is that 60% of all email with Sender ID Framework records fails authentication. IronPort's SenderBase analysis of authentication failures revealed 1 in 8 messages

failing authentication came from a positive reputation source, the others were of neutral or poor reputation. The messages that successfully authenticated were overwhelmingly legitimate with only 1 in 20 being spam.

What's Working and What's Not—Noteworthy Conclusions

- Very little spam passes authentication checks. This result contradicts early studies that showed spammers were leading Sender ID Framework adopters.
- A weak correlation exists between spam and email that fails Sender ID Framework authentication or lacks a published record. This is primarily due to almost 50% of all Sender Policy Framework (SPF) failures originating from “neutral” sources of email – forwarders and domains which send primarily legitimate email but have some spam as well.
- Positive reputation sources of email that pass authentication checks are very strongly correlated with legitimate email, enabling whitelisting and positive factors in spam scoring systems.
- Reputation is critical to extracting value from SPF data. The utility of SPF results increase tenfold when correlated with reputation data.
- The largest barrier to Sender ID Framework impact is authentication failures of legitimate messages. The reasons for an authentication failure are myriad. For example, forwarded mail can easily break common authentication implementations today. There may also be unknown sources of legitimate email not published in the SPF/Sender ID record.

IronPort's Dedication to Fixing Email

Underscoring its dedication to fixing email, IronPort joins other industry leaders in urging industry-wide adoption of authentication standards. IronPort was the first to introduce an email appliance that integrated DomainKeys to fight email fraud, protect online consumers, and secure business' identity on the Internet. IronPort also supports the use of SPF/Sender ID. IronPort is pleased to be an underwriter of the Email Authentication Implementation Summit 2005. For more information visit <http://emailauthentication.org/summit2005/>.

ABOUT IRONPORT SYSTEMS

IronPort Systems is the leading email security provider for organizations ranging from small businesses to the Global 2000. The company has developed a family of email security appliances, the IronPort C-Series™, that offer breakthrough performance, unprecedented ease of use and reduced total cost of ownership. IronPort is driving new standards and providing innovative products for those faced with the monumental task of managing, protecting, and growing mission-critical email systems. For more information on IronPort products and services, visit: <http://www.ironport.com>.

###