



## SECURITY WORLD 2009

*“SECURE your organization in an INSECURE era”*

### NETWORK SECURITY & DATA PROTECTION

#### **Data Security-Experience sharing from VietinBank**

*Mr. Nguyen Anh Tuan, Manager, The Research and Development Dept., IT Center, Vietinbank*

Not until recently has data protection been spotlighted in Vietnam. This presentation will bring analysis on the following issues:

- What is the importance of data protection in the overall enterprises' security systems?
- What are the threats to enterprises' data?
- What are principles and solutions for effective data protection?
- Successful practices at Vietinbank

Different types of databases, from databases of certain structures to non-structural; from private end-user to complex enterprises' databases, etc will also be discussed in this presentation.

#### **Architecture of High End Network Encryption Products – High end Encryption Solutions for the Governments**

*Mr. Georg Krause, Founder & CEO, CE-Infosys*

Network encryption products are widely used nowadays to create virtual private networks within a public network infrastructure, for ministries, military organisations and other bodies. Large amounts of information, some highly sensitive, are encrypted with these devices, and transmitted to other sites. As such, the security of these devices are of utmost importance. However, the selection criteria of these devices usually weigh heavily towards ease of operation and maintenance. Unknown to many during the selection phase, it is relatively simple to defeat a network encryption device especially if it is poorly designed, as can be seen in the recent Princeton research. In this presentation, we will be describing the Advanced Network Infrastructure Security (ANIS) architecture designed by CE-Infosys. This architecture is ideal for top security for Governments, so and can securely protect the confidentiality of the data on their critical networks. With a recent trend of cyberwarfare and cyberterrorism, the security of these networks is paramount, so that a country can continue to function in the face of these attacks.

## **PALI – PineApp Lawful Interception Technology Overview**

*Mr. David Feldman, VP Technical Services, PineApp*

Lawful interception is the interception of telecommunications by law enforcement agencies (LEA's) and intelligence services, in accordance with local law and after following due process and receiving proper authorization from competent authorities.

The biggest challenge in email lawful interception resides in the fact that more than 90% of email traffic is invalid: Spam, Phishing, Viruses and many other email-borne threats.

Due to this fact, it has become almost impossible to extract information in real-time as most of the processing time is wasted on analyzing irrelevant content. To make it even harder, using standard anti-spam/anti-virus devices is impossible since the listened email traffic is not directed to the unit (a crucial condition for such devices to function properly), but rather “captured” using a “tapping” device.

Based on the award winning Mail-SeCure™ product, PineApp Lawful Interception Solution – PALI™ – offers a comprehensive yet flexible end-to-end solution for any infrastructure, filtering all the non-relevant content, thus providing pinpointed and accurate processing of the relevant information or lawful interception needs. Furthermore, Mail-SeCure enables real-time content analysis of mail traffic, in-addition or instead of existing content extraction systems.

This presentation introduces PALI solution, and highlights various technological aspects of the solution's work methods.

## **The Center is everywhere**

*Mr. Wong Kang Yeong, Regional Security Architect, ASEAN, SonicWALL, Inc.*

Datacenters continue to power IT services that is unleashed to mobile users and road warriors. With Internet-enabled mobile devices and wireless connectivity, it's a breeze for executives to reply to emails, access important business information from company servers without having to be physically in the office.

However convenience on the go also comes with potential liability – security. When I send sensitive and confidential information to my clients over a wireless network, I expect secure delivery without worry that the information will fall into the wrong hands.

Sonicwall shall share strategies to secure these IT resources and its mobile users in this session.