XSP Security Vulnerabilities Panel
NANOG 34 - Seattle, WA
15 MAY 2005

Martin Hannigan

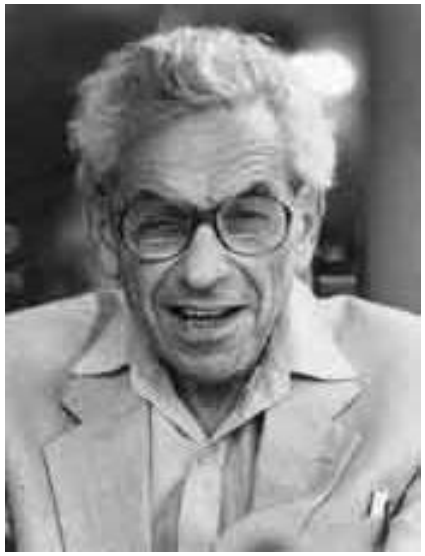
Network & Security Architecture Group

Where it all comes together.

Abstract

- **Increased threats and security demands by customers and the Operator community have led to pressure on Operators and Providers to provide a more secure Internet.**
- **This panel will examine network related vulnerability issues and their impact on the Internet operational community at large.**
- **There is a plan for a panel at NANOG 35 to address Disclosure methods.**

Famous Quote



"Problems worthy of attack prove their worth by fighting back."

- Paul Erdos, Mathematician (1913-1996)

Introductions

- **Patrick W. Gilmore** is Director of Network Strategy & Support at Akamai Technologies, where he has worked for the last 5 years helping to build the largest Content Distribution Network in the world. Patrick has experience with large network design and deployments in both the ISP and enterprise spaces. Prior to working at Akamai, Patrick was Chief Network Architect for Onyx Networks. Before that he worked for Concentric Networks, and as Director of Operations at Priori Networks.

Intro (2)

- **Martin Hannigan**, **(moderator)** is a member of the Networks and Security Architecture staff at VeriSign, a provider of Intelligent Infrastructure services. Prior to VeriSign, Martin's 18 years of experience includes many firsts in the industry: The first Internet Privacy Policy, SS7 bypass as a predecessor to soft-switching, Intelligent Agent software for high profile web sites, and the intelligent directory services of Microsoft Passport. He's been responsible for facility design, build out, and network implementation at Level(3) Communications, Director of Engineering and Operations at InterNAP, CALEA Architect at CTC Communications, and past Manager of the VeriSign Security Services "SOC".

Intro (3)

- **Aaron Hughes**, is currently the Vice President of Technology at Terremark Worldwide, Inc., a leading operator of Internet exchange points (IX). Mr. Hughes is responsible for all network and system topology planning and design. Prior to joining Terremark, Mr. Hughes was Vice President of Operations at YellowBrix., where he led operations, sales engineering, planning and design. Mr. Hughes has held network and system architecture roles at Certainty Solutions, Quest Technologies, RCN, UltraNet and Channel(1) Communications.

Intro (4)

- **Chris Malayter** is a Data Network Engineer at TDS Telecom in Madison, WI. He has held a number of roles at TDS. In his current position, his team is responsible for designing and engineering the data networks that comprise TDS' Internet business. Chris was a primary player in the recent redesign of the TDS nationwide core network. In addition, he is responsible for all Internet peering coordinator at TDS Telecom

Intro (5)

- **Chris Morrow** has been a Network Security Engineer at UUNET/MCI for 5 years, while actually being a Chemical Engineer in real-life. While at UUNET/MCI he has been responsible for a team of engineers helping to mitigate DoS attacks against UUNET/MCI Customers. Additionally, he's been responsible for evaluating new security issues for relevance to the UUNET/MCI Public IP backbone and other MCI networks.

Intro (6)

- **Richard Steenbergen** is the Founder of nLayer Communications, where he currently serves as Chief Technical Officer. Previously, he served as a Sr. Network Engineer for several large NSPs, and was the Sr. Software Engineer developing advanced routing technologies at netVmg, Inc.

Commentary: Jerry Dixon

- **Jerry Dixon** is Deputy Director of Operations for the National Cyber Security Division's, U.S. Computer Emergency Readiness Team (US-CERT). Prior to joining NCSD, he was the founding director of the Internal Revenue Service's Computer Security Incident Response Capability including having served as Director of Information Security for Marriott International, a global private sector company. Mr. Dixon is currently a Certified Information Systems Security Professional and actively engaged with public and private sector efforts in the information security community.

Commentary: Prof. Robert Mathews

- **Prof. Mathews** is a Distinguished Senior Research Scholar on National Security Affairs and U.S. Industrial Preparedness at the University of Hawai'i. A domain specialist in ultra-complex systems, Prof. Mathews' professional concentrations over the past 3 decades include non-linearity in highly distributed - large scale systems, and emergent behaviour as those found in Command, Control, Communications, Intelligence, Surveillance and Reconnaissance (C3ISR) systems. Additionally, he serves as senior policy and programs analyst to the U.S. government on a variety of national security matters, which include U.S. critical infrastructures, national technical assets, the intelligence community, counter-terrorism and domestic security. Prof. Mathews holds advanced degrees in both Management and Economics.

Security Panel (1)

QUESTION:

- **If one company discovers a vulnerability and the impact is in its infancy, is it worth announcing it to all customers and/or the Operator community?**
- **Does that create a larger vulnerability?**

Security Panel (2)

QUESTION:

- **Is announcing a vulnerability putting tools into (script kiddies/hackers/angry people's) hands and could this be prevented?**
- **Should vulnerability announcements be restricted to a selective group to prevent this?**

Security Panel (3)

QUESTION:

- **What if routers, switches, and network-objects had a 'smart update‘ feature much like windows-update or Software Update (for you Apple users)? Would this end the continuous and massive spreads of viruses, irc bots, and open relays, and could the average enterprise deal with a regular 3am reload (~5 min outage)?**

Security Panel (4)

"As Code Red and Nimda have proven, blended threats can wreak havoc on enterprise security because they evolve more rapidly, are progressively more complex, and occur more frequently than past attack methods. The worst threats are likely yet to come."

- **Why are the most affected companies, enterprises, not managing bug fixes and vulnerabilities until they are reacting to an attack?**
- **Is it too hard to manage changes?**
- **Are network engineers simply too expensive?**
- **Has marketing led enterprises to believe we are living in a self healing world?**

Security Panel (5)

On April 20, 2004, a vulnerability was found in MD5. Service Providers were required to react swiftly to enable passwords on BGP sessions globally

QUESTION:

- **If there is a "work around" available before the software fix is in (e.g. BGP/MD5), should it be announced publicly before the vulnerability, or should affected parties be notified privately?**

Security Panel (6)

There are multiple methods of vulnerability announcements that impact the Operator community. Those include "the whisper network", NSP-SEC, NANOG, and INOC-DBA, and vendor reporting methods like PSIRT.

QUESTION:

- **What is the most expedient path to get the information to ISP's to collaboratively determine mitigations in the absence of a patch?**
- **Would we feel compelled to share mitigation of the same outside of the US region?**
- **Is the "whisper network" good or bad?**

At the Microphone

- **Jerry Dixon, DHS NCSD US-CERT**
  - **What role should the Department of Homeland Security/US-CERT have resolving issues surrounding vulnerability release?**
- **Prof. Robert Mathews, University of Hawai'i**
  - **In a GLOBAL NETWORK OPERATOR community, one has certain local responsibilities specificially, and certain communal responsibilities at the global level; both of which are essential PARTS of a responsible PRACTITIONER'S manual. In an operational context, what are the distinct boundaries/major themes for each area as we understand and accept universally?**

Closing

QUESTIONS OR COMMENTS?

THANK YOU!

References:

Question 6: Institute of Internal Auditors *www.thelia.org