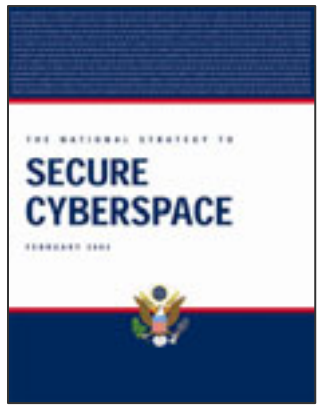
U.S. Government Concerns with the Routing Infrastructure

ARIN
Los Angeles, CA
October 27, 2005

Douglas Maughan, Ph.D.
Program Manager, HSARPA
douglas.maughan@dhs.gov
202-254-6145 / 202-360-3170

Internet Infrastructure Security

- The National Strategy to Secure Cyberspace (2003) recognized the DNS as a critical weakness
  - NSSC called for the Department of Homeland Security to coordinate public-private partnerships to encourage the adoption of improved security protocols, such as DNS and BGP.
  - **The security and continued functioning of the Internet will be greatly influenced by the success or failure of implementing more secure and more robust BGP and DNS**. The Nation has a vital interest in ensuring that this work proceeds. **The government should play a role when private efforts break down due to a need for coordination or a lack of proper incentives.**



Secure Protocols for the Routing Infrastructure (SPRI)

- Work with industry to develop solutions for the current routing security problems and develop technologies for the future

- The first workshop in the series (Workshop 1: Security Requirements) was held Mar 15-16, 2005, in Arlington, VA, with attendees from the ISP operator, security, and government communities. The goal of the Security Requirements workshop was to come to a common understanding of the real security problems that need to be solved to improve the routing infrastructure. Position papers and a workshop summary are available at http://www.hsarpacyber.com/public/spri/workshop1.

SPRI Progress (continued)

- The second workshop in the series (Workshop 2: Engineering and Operational Requirements for Security Solution) was held May 18-19, 2005, in Seattle, WA, following NANOG. The focus of the workshop was to gather input from the service provider community about their constraints, issues, and procedures of operations that must be considered in developing a useable, deployable security technique. Presentations and a draft summary of that workshop are presently available at http://www.hsarpacyber.com/public/spri/workshop2.

- Identified critical areas associated with the Regional Internet Registries (RIRs) and the ISP requirements of those registries, including the data available from the registries and how the ISPs use this data.

SPRI Workshop #3

- The third workshop in the series (Workshop 3: Requirements of Routing Registries) was held Sept 13-14, 2005, in Washington, DC.
- The Goals for workshop #3 were:
  - Better understanding of the RIR "business" and the information they collect (and don't collect)
  - Opportunity for discussion between ISPs and RIR about additional information needed to support ISPs in order to do their job
  - Better understanding of the registry database schemas and the information available to customers/users
  - Identification of key points to improve information access for registry customers
- Presentations and a draft summary of that workshop will be available at http://www.hsarpacyber.com/public/spri/workshop3.

U.S. Government Concerns

- Lack of authentication on prefix assignment
- Lack of authentication on ASN assignment
- Absence of processes to provide authenticated AS/prefix mapping
- Absence of processes and data to document sub-allocations
- Legacy space issues

U.S. Government Suggestions

- Create a robust routing information infrastructure of sufficient quality to enable new levels of automation of:
  - Maintenance of ISP/Customer Relationships
  - Managing Local Policies
  - Supporting Secure Routing Mechanisms
    - Peer Authentication.
    - Prefix Origin Authentication.
    - Route / Path Authentication.
  - Improving Diagnostics and Anomaly Detection.
- Define the technical requirements for tools / services to address the information quality issues with new / existing RIR / IRR data.

Homeland Security

Douglas Maughan, Ph.D.

Program Manager, HSARPA

douglas.maughan@dhs.gov

202-254-6145 / 202-360-3170

Homeland Security

Homeland Security