Internet and Scalable Systems Research

Addressing Systemic Challenges to Our Network Centric Society

Doug Montgomery (dougm@nist.gov)
Internet and Scalable Systems Metrology Group
Advanced Network Technologies Division
Information Technology Laboratory
http://www.anld.nist.gov/
Evolving the Core Infrastructure of the Internet

- **Internet technologies** provide a technical basis for most systems (information, transportation, manufacturing, communications, defense, Government, education, etc) vital to our nation.

- **The Internet is at a cross roads** as the viability of several of its most basic infrastructural technologies (routing, naming, and addressing) are threatened by inherent robustness vulnerabilities and scaling problems.

- **NIST is engaged in three critical efforts** aimed at fundamentally changing the structure/services of the Internet to address these threats:
  - Internet Infrastructure Protection (IIP).
  - Next Generation Internet Technologies (NGI).
Fostering Real Change

• If you *only* standardize it ... they won’t come.
  - How do you get changes to the infrastructure deployed?

• The National Strategy to Secure Cyberspace
  - “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.

• NIST ISSMG Goals: To change the Internet.
  - Carrots – problem identification, research, designs, tests, measurements, standards, testbeds, prototypes, deployment guidance, training, outreach.
  - Sticks – FISMA reqs/auditing procedures, tech basis for other USG policies, FAR, FIPS.
ISSMG Mission / Competencies

• **Fostering New Network Technology** - The ISSMG works with industry to improve the quality and timeliness of emerging specifications and early implementations of next-generation Internet technologies and distributed information systems.

• **Advancing Network Metrology** - The emphasis of the group is on innovating and applying advanced measurement science to increase the robustness and expand the applicability of potentially disruptive Internet technologies.

• **Competencies** of the group include: modeling and analysis of emerging Internet technologies, measurement science for scalable information systems, design and evaluation of advanced network test and measurement techniques, and rapid prototyping and empirical measurement of early protocol designs.

• Our efforts focus on **Internet Scale problems, solutions and measurement techniques**.
Need for NIST?

• Understanding / Controlling Network Behavior
  – “[Despite] society’s profound dependence on networks, fundamental knowledge about them is primitive. [G]lobal communication … networks have quite advanced technological implementations but their behavior under stress still cannot be predicted reliably…. There is no science today that offers the fundamental knowledge necessary to design large complex networks [so] that their behaviors can be predicted prior to building them.”

  Network Science 2006, a report from the National Research Council.

• Cost of our current inability:
  – “Cost of eBay's 22-Hour Outage Put At $2 Million”, Ecommerce, Jun 1999
  – “Last Week’s Internet Outages Cost $1.2 Billion”, Dave Murphy, Yankee Group, Feb 2000
  – “…the Internet “basically collapsed” Monday”, Samuel Kessler, Symantec, Oct 2003
  – “Network crashes…cost medium-sized businesses a full 1% of annual revenues”, Technology News, Mar 2006
  – “costs to the U.S. economy…range…from $65.6 M for a 10-day [Internet] outage at an automobile parts plant to $404.76 M for … failure …at an oil refinery”, Dartmouth study, Jun 2006

  – Risks of deliberate attack even greater….
What are NIST’s Roles?

- Problem Identification
- Requirements Analysis
- Threat Modeling
- Problem Space Characterization
- Consensus Standards
- Protocol Design
- Protocol Prototypes & Models
- Deployment Guidance
- FIPS / FISMA Requirements
- Tests and Measurements
- Pilot Testbeds
- Metrology
- Develop Technical Basis For Policy
- Deployment Guidance

Define USG R&D Priorities

NIST Advanced Networking Technologies Division

8/17/16
ISSSMG Techniques

• **Analytical, Simulation & Emulation Modeling.**
  – Internet scale modeling for performance, scalability, vulnerability, robustness.

• **Protocol Design and Analysis.**
  – Internet Engineering Task Force (IETF).

• **Internet Scale Measurement and Data Analysis.**
  – Measurement and monitoring of Internet infrastructure.
  – Collaboration with various large scale measurement activities.

• **Rapid Prototyping.**
  – Open source reference implementations of emerging specifications.

• **Deployment guidance / profiles.**
  – Fostering commercial acquisition and deployment

• **Product Testing and Evaluation**
  – Test tools designed to assist implementers and early adopters.
  – Accredited testing laboratories for formal product interoperability and conformance.
ISSSMG Projects

• Robust Inter-Domain Routing – Working with industry to improve global Internet routing security and robustness, Border Gateway Protocol (BGP), measurement monitoring and analysis of global BGP behavior, BGP security and performance issues, and next generation routing architectures.

• High-Assurance Domains – Research and develop Domain Name System (DNS) technologies, DNSSEC security protocols, IETF DANE technologies to leverage the DNS as a key discovery and management infrastructure, use of DANE and other DNSSEC enabled technologies, X.509/PKIX certificate technologies, TLS / SSL implementation, and SMIME / PGP email security protocols.

• Network Anomaly Detection / Synthetic Traffic Generation – Research and develop measurement science to advance the state of the art in network anomaly detection, network intrusion detection, synthetic traffic generation, statistical modeling of network traffic, machine learning, test and instrumentation of NAD/NID systems.
ISSSMG Projects

- **Software Defined Virtual Networks** – Develop test and measurement techniques to advance the state of the art in network virtualization, network service function chaining, software defined networks, technologies and techniques to address robustness safety and security of virtualized network services. Explore novel applications of NFV/SDN to domains such as network security and intrusion detection, support of machine to machine communications, support of advanced mobility and cloud computing.

- **Measurement Science of Complex Networks** - Research and develop of techniques to measure, predict and control macroscopic / emergent behavior in complex information systems, modeling and analysis techniques to characterize Internet scale networks and distributed systems, use of genetic algorithms to search for rare events, and runtime techniques to predict phase transitions in system behavior.
ISSMG Projects

- **Advanced DDoS Mitigation Techniques** – Working with DHS S&T and industry to research and develop novel approaches to DDoS detection and mitigation, techniques to test and measure the effectiveness and impact of DDoS / spoofing mitigation techniques, develop deployment guidance for such techniques.

- **USGv6** – Working with other USG agencies and industry to develop and maintain the standards, test program, deployment guidance and test and measurement tools necessary to provide the technical underpinnings for wide scale adoption of IPv6 in the USG.
Details on Select Projects
IIP – Robust Inter-domain Routing

• **Objective:** Working with industry to improve global Internet routing robustness, Border Gateway Protocol (BGP), measurement monitoring and analysis of global BGP behavior, BGP security and performance issues, and next generation routing architectures.

• **Select Accomplishments:**
  – IRTF Next Generation Routing Architecture - [https://irtf.org/concluded/rrg](https://irtf.org/concluded/rrg)
  – IETF Secure Inter Domain Routing - [https://datatracker.ietf.org/wg/sidr/](https://datatracker.ietf.org/wg/sidr/)
  – NIST BGP SRx - [http://www-x.antd.nist.gov/bgpsrx/](http://www-x.antd.nist.gov/bgpsrx/)
  – BRITE - [https://brite.antd.nist.gov/](https://brite.antd.nist.gov/)

• **Plans:**
  – Standards – complete IETF BGPSEC RFC
  – Prototypes – complete and test BGP-SRX
  – Measurement – research and develop “big data” tools for BGP anomaly detection.
  – Tools – update BGPSEC test tools to final spec.

• **Collaborators:**
  – IETF, IRTF, DHS S&T, BBN, Google, IIJ, Parsons, Cisco, Juniper, NANOG.
IIP – High Assurance Domains

• **Objective:** Research and develop Domain Name System (DNS) technologies, DNSSEC security protocols, IETF DANE technologies to leverage the DNS as a key discovery and management infrastructure, use of DANE and other DNSSEC enabled technologies, X.509/PKIX certificate technologies, TLS / SSL implementation, and SMIME / PGP email security protocols.

• **Select Accomplishments:**
  – IETF DANE - [https://datatracker.ietf.org/wg/dane/](https://datatracker.ietf.org/wg/dane/)
  – NCCOE DNS-Based Secure Email - [https://nccoe.nist.gov/projects/building_blocks/secured_email](https://nccoe.nist.gov/projects/building_blocks/secured_email)
    • Testers for DANE enabled TLS, SMTP, SMIME and DMARC/DKIM/SPF deployment.

• **Plans:**
  – Support NCCoE project, complete SP, enhance and deploy test tools.

• **Collaborators:**
  – IETF, M3AAWG, NCCOE, Verisign, Secure64, Microsoft, Comcast, ISC, …
NGI – Software Defined Virtual Networks

• **Objective:** Develop test and measurement techniques to advance the state of the art in network virtualization, network service function chaining, software defined networks, technologies and techniques to address robustness safety and security of virtualized network services. Explore novel applications of NFV SDN to domains such as network security and intrusion detection, support of machine to machine communications, support of advanced mobility and cloud computing.

• **Select Accomplishments:**
  – SDN / NFV Testbed – testbed of hardware / software SDN/NFV implementations and test tools.

• **Plans:**
  – Development measurement / benchmarking techniques for SDN controllers and switches
  – R&D programmable measurement techniques for SDN and their application to DDoS detection and mitigation.
  – Formal analysis of OVS softswitch implementations.

• **Collaborators:**
  – GMU, NSA, UNH IOL, ONF,
NGI – USGv6 Program

• **Objective:**
  – OMB Memorandum M-05-22 directed the National Institute of Standards and Technology (NIST) to develop the technical infrastructure (standards and testing) necessary to support wide scale adoption of IPv6 in the US Government (USG). In response NIST developed a technical standards profile for US Government acquisition of IPv6 Hosts and Routers, and a specification for Network Protection Devices. The USGv6 profile includes a forward looking set of RFCs published by the Internet Engineering Task Force (IETF), encompassing basic IPv6 functionality, and specific requirements and key optional capabilities for routing, security, multicasting, mobility, network management, and quality of service. The profile also contains a NIST established set of capability requirements for IPv6 aware firewalls and intrusion detection systems. In addition to the profiles, a testing program has been established to enable products to be tested for compliance with the profile by accredited laboratories.

• **Select Accomplishments:**
  – NIST SP 500-273 *USGv6 Test Methods: General Description and Validation.*

• **Plans:**
  – Complete version 2 of the USGv6 profile and continue to evolve the testing program

• **Collaborators:**
  – UNH IOL, Fed V6 Task Force, OMB, GSA.
CxS – Measurement Science for Complex Networked Information Systems

**Objective:** Research and develop of techniques to measure, predict and control macroscopic / emergent behavior in complex information systems, modeling and analysis techniques to characterize Internet scale networks and distributed systems, use of genetic algorithms to search for rare events, and runtime techniques to predict phase transitions in system behavior.

**Select Accomplishments:**

**Plans:**
- Complete / publish research on influence of realism in network simulations.
- Investigate validation techniques for simulations of large-scale networks.
- Research runtime methods for predicting failures in networked information systems.

**Collaborators:**
8/17/16
NIST Advanced Networking Technologies Division
ISSMG Collaborations

- SDOs / IGOs
- Consortia / Groups
- Industry
- USG
Questions?

dougm@nist.gov