The Role of Testbeds in Cyber Security Research

CSET
Washington, DC
August 9, 2010

Douglas Maughan, Ph.D.
Branch Chief / Program Mgr.
douglas.maughan@dhs.gov
202-254-6145 / 202-360-3170

Homeland Security

Definition - Wikipedia

- **Testbed** is **a platform for experimentation** of large development projects. Testbeds allow for **rigorous, transparent, and replicable testing** of scientific theories, computational tools, and new technologies.
- The term is used across many disciplines to describe a development environment that is **shielded from the hazards of testing in a *live* or production environment**. A testbed is used as **a proof of concept** or when a new module is tested apart from the program/system it will later be added to.
- A **typical** testbed could include software, hardware, and networking components, and can also be known as the test environment.

The Internet: The Ultimate Testbed

"The ARPANET came out of our frustration that there were only a limited number of large, powerful research computers in the country, and that many research investigators, who should have access to them, were geographically separated from them."

Charles Herzfeld

Other Testbeds: 1980s to early 2000s

- National Science Foundation (NSF)
  - CSNET - "Computer Science Network" developed in the early 1980s that linked computer science departments at academic institutions
  - NSFNET - An open network allowing academic researchers access to supercomputers. NSFNET went online in 1986.
  - vBNS - Project to provide high-speed interconnection between NSF-Sponsored supercomputing centers and select access points. The network was engineered and operated by MCI Telecommunications.
- DARPA
  - DARTNET – DARPA Research Testbed NETwork
  - CAIRN - An internetwork testbed network to demonstrate new high-speed transmission technologies and to support a variety of Computer Science research, primarily intended as a testbed for advanced computer network protocols research and development. The most salient characteristic of CAIRN is: "a network we can break".

Homeland Security

More recent testbeds - ORBIT

- A two-tier laboratory emulator/field trial **wireless network testbed** designed to achieve reproducibility of experimentation, while also supporting evaluation of protocols and applications in real-world settings
- A novel approach involving a large two-dimensional grid of 400 802.11 radio nodes which can be dynamically interconnected into specified topologies with reproducible wireless channel models
- The testbed is available for remote or on-site access by other research groups nationally. Additional research partners and testbed equipment/software **contributors are actively sought** from both industry and academia.

Homeland Security

More recent testbeds - GENI

- Global Environment for Network Innovations
- A virtual laboratory for exploring future internets at scale, creates major opportunities to understand, innovate and transform global networks and their interactions with society. GENI will:
  - support at-scale experimentation on shared, heterogeneous, highly instrumented infrastructure;
  - enable deep programmability throughout the network, promoting innovations in network science, security, technologies, services and applications; and
  - provide collaborative and exploratory environments for academia, industry and the public to catalyze discoveries and innovation
- Core concepts: Programmability, Virtualization and Other Forms of Resource Sharing, Federation, and Slice-based Experimentation.

Homeland Security

More recent testbeds - NCR

- NCR = National Cyber Range
- GOAL: Enable a revolution in the Nation's ability to conduct cyber operations by providing a persistent cyber range that will facilitate the following:
  - Conduct unbiased, quantitative and qualitative assessment of information assurance and survivability tools in a representative network environment.
  - Replicate complex, large-scale, heterogeneous networks and users in current and future architectures and operations.
  - Enable multiple, independent, simultaneous experiments on the same infrastructure.
  - Develop and deploy revolutionary cyber experiment capabilities.
  - Enable the use of the scientific method for rigorous cyber experiments.

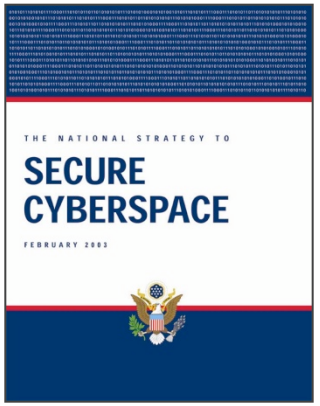
Science and Technology (S&T) Mission

Conduct, stimulate, and enable **research, development, test, evaluation and timely transition** of homeland security capabilities to federal, state and local operational end-users.

Homeland Security

National Strategy to Secure Cyberspace

- The National Strategy to Secure Cyberspace (2003) recognized the Domain Name System (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 – **DNSSEC Deployment Coordination Initiative**
  - **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.**



Homeland Security

DNSSEC Initiative Activities

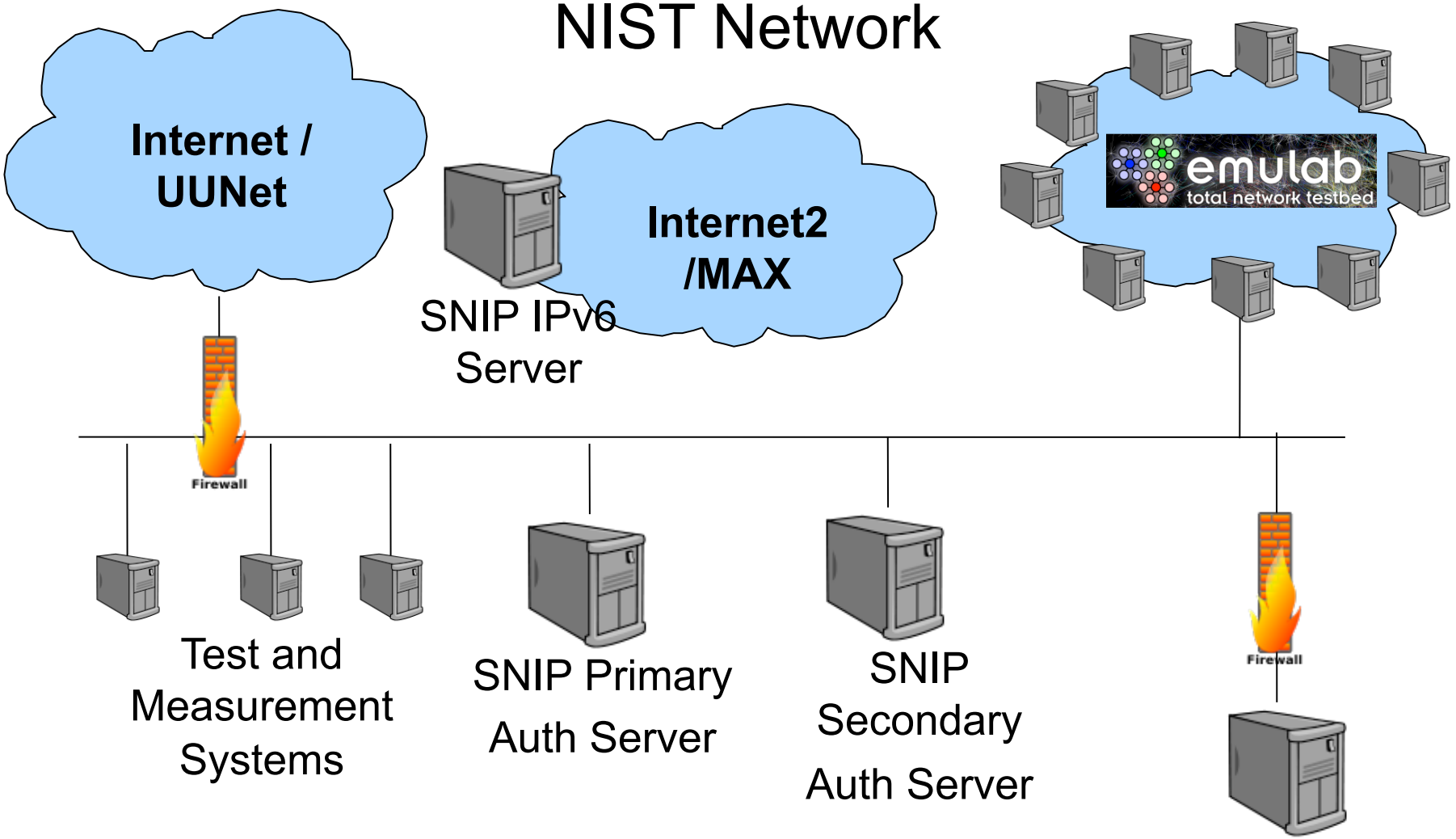
- Roadmap published in February 2005; Revised March 2007
  - http://www.dnssec-deployment.org/roadmap.php
- Multiple workshops held world-wide
- Involvement with numerous deployment pilots
- **DNSSEC testbed developed in partnership with NIST**
  - http://www.dnsops.gov/
- Formal publicity and awareness plan including newsletter, blog, wiki
  - http://www.dnssec-deployment.org/
- **Working with Civilian government (.gov) to develop policy and technical guidance for secure DNS operations and beginning deployment activities at all levels**
- Working with vendor community and others to promote DNSSEC capability and awareness in their software or projects

Homeland Security

Secure Naming Infrastructure Pilot (SNIP)

- SNIP is a USG (and others) DNS Ops community and shared pilot
  - Provide "distributed training ground" for .gov operators deploying DNSSEC
  - Ability to pilot agency specific scenarios either locally or in SNIP-provided resources.
  - Create a community resource for DNS admins in the USG to share knowledge and to refine specifications, policies and plans.
- SNIP basis is a signed shadow zone under .gov (dnsops.gov)
  - Offers delegations and secure chaining to subzones
    - For example – NIST participates as nist.dnsops.gov

SNIP Topology
NIST Network



Homeland Security

SNIP Impact

- Stepping stone for operational use
  - USG DNS operators get experience running delegation under dnsops.gov before deploying in own agency
- Tool testing
  - Tech transfer / training on existing tool suites (NIST, SPARTA, Shinkuro, ISC, et al).
- Platform Testing
  - Multi-vendor environment
    - Servers - ISC/BIND, NSD, Secure64, Windows Server 2008 R2, etc.
    - Resolvers – Linux, BSD, Microsoft, OS X.
- Procedure Testing
  - Refinement of procedure/policy guidance and reporting requirements
  - All results will form the basis of NIST SP 800-81r1

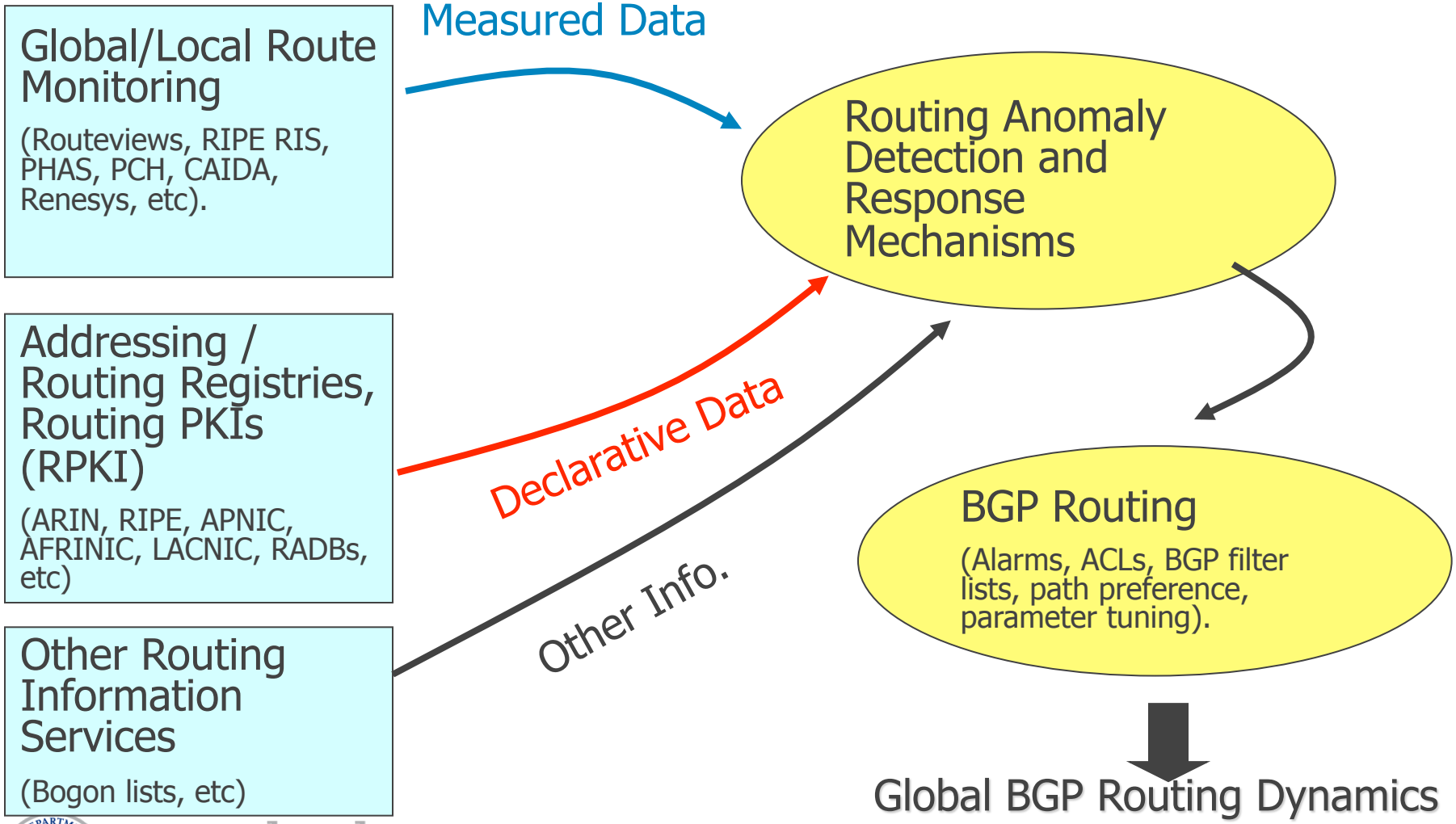
History of Routing Outages

- Commercial Internet -- specific network outages
  - Apr 1997 – AS 7007 announced routes to all the Internet
  - Apr 1998 – AS 8584 mis-announced 100K routes
  - Dec 1999 – AT&T's server network announced by another ISP – misdirecting their traffic (made the Wall Street Journal)
  - May 2000 – Sprint addresses announced by another ISP
  - Apr 2001 – AS 15412 mis-announced 5K routes
  - Dec 24, 2004 – thousands of networks misdirected to Turkey
  - Feb 10, 2005: Estonian ISP announced a part of Merit address space
  - Sep 9, 2005 – AT&T, XO and Bell South (12/8, 64/8, 65/8) misdirected to Bolivia [the next day, Germany – prompting AT&T to deaggregate]
  - Jan 22, 2006 – Many networks, including PANIX and Walrus Internet, misdirected to NY ISP (Con Edison (AS27506))
  - Feb 26, 2006 - Sprint and Verio briefly passed along TTNET (AS9121 again?) announcements that it was the origin AS for 4/8, 8/8, and 12/8
  - Feb 24, 2008 –Pakistan Telecom announces /24 from YouTube
  - March 2008 – Kenyan ISP's /24 announced by AboveNet
  - Frequent full table leaks, e.g., Sep08 (Moscow), Nov08 (Brazil), Jan09(Russia)

Secure Protocols for the Routing Infrastructure (SPRI)

- Border Gateway Protocol (BGP)
  - Routing protocol that connects ISPs and subscriber networks together to form the Internet; Exchanges network *reachability information*
  - Final version: BGP-4 (RFC 1771-1774 – 3/95)
- The BGP architecture makes it highly vulnerable to human errors and malicious attacks against
  - Links between routers
  - The routers themselves
  - Management stations that control routers
- Working with global registries to deploy Public Key Infrastructure (PKI) between ICANN/IANA and registry and between registry and ISPs/customers
- Working with industry (router vendors, ISPs) to develop solutions for our current problems and future technologies

Solution Components / Players



Homeland Security

Test & Measurement Challenges

Global/Local Route Monitoring

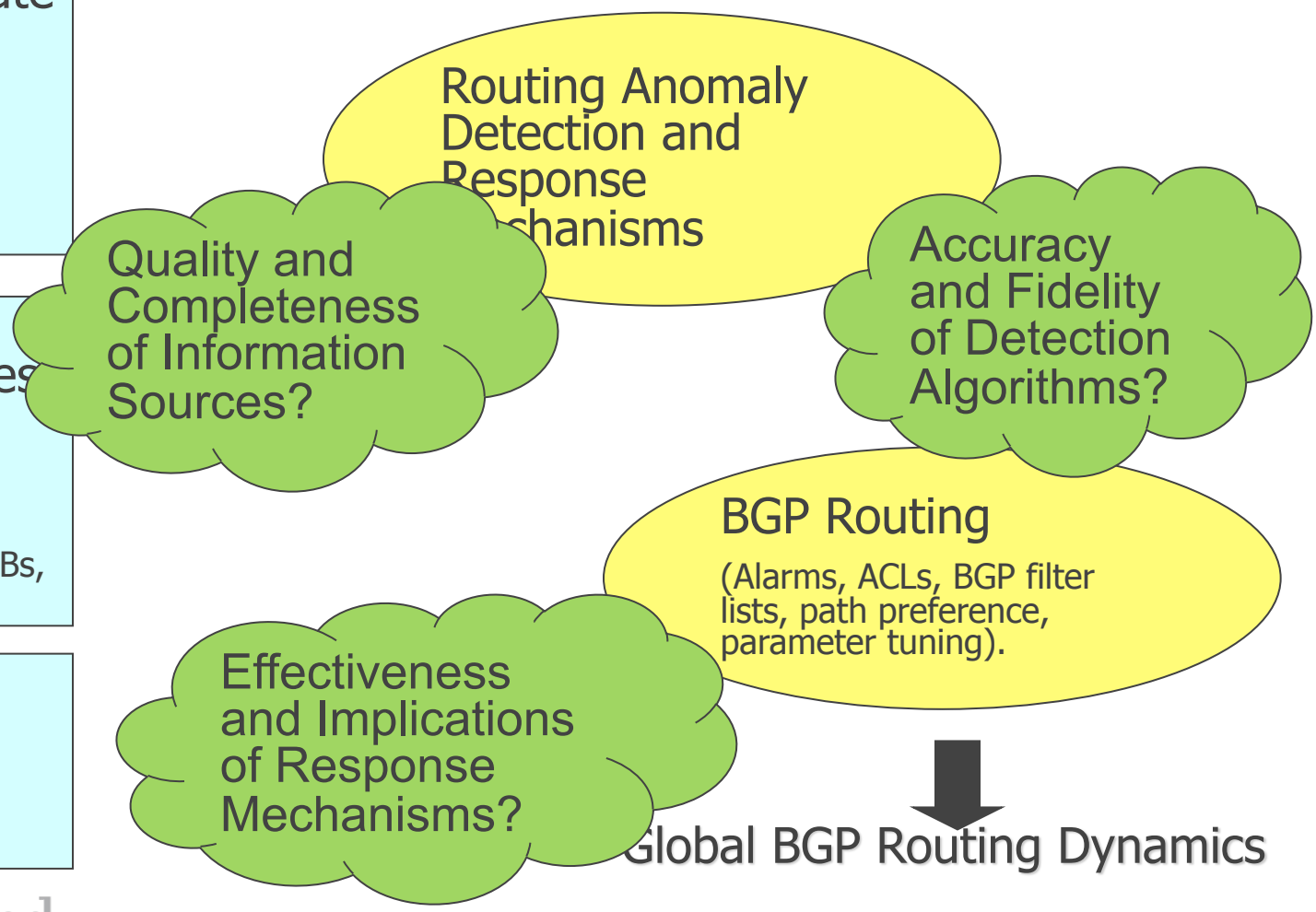
(Routeviews, RIPE RIS, PHAS, PCH, CAIDA, Renesys, etc).

Addressing / Routing Registries Routing PKIs (RPKI)

(ARIN, RIPE, APNIC, AFRINIC, LACNIC, RADBs, etc)

Other Routing Information Services

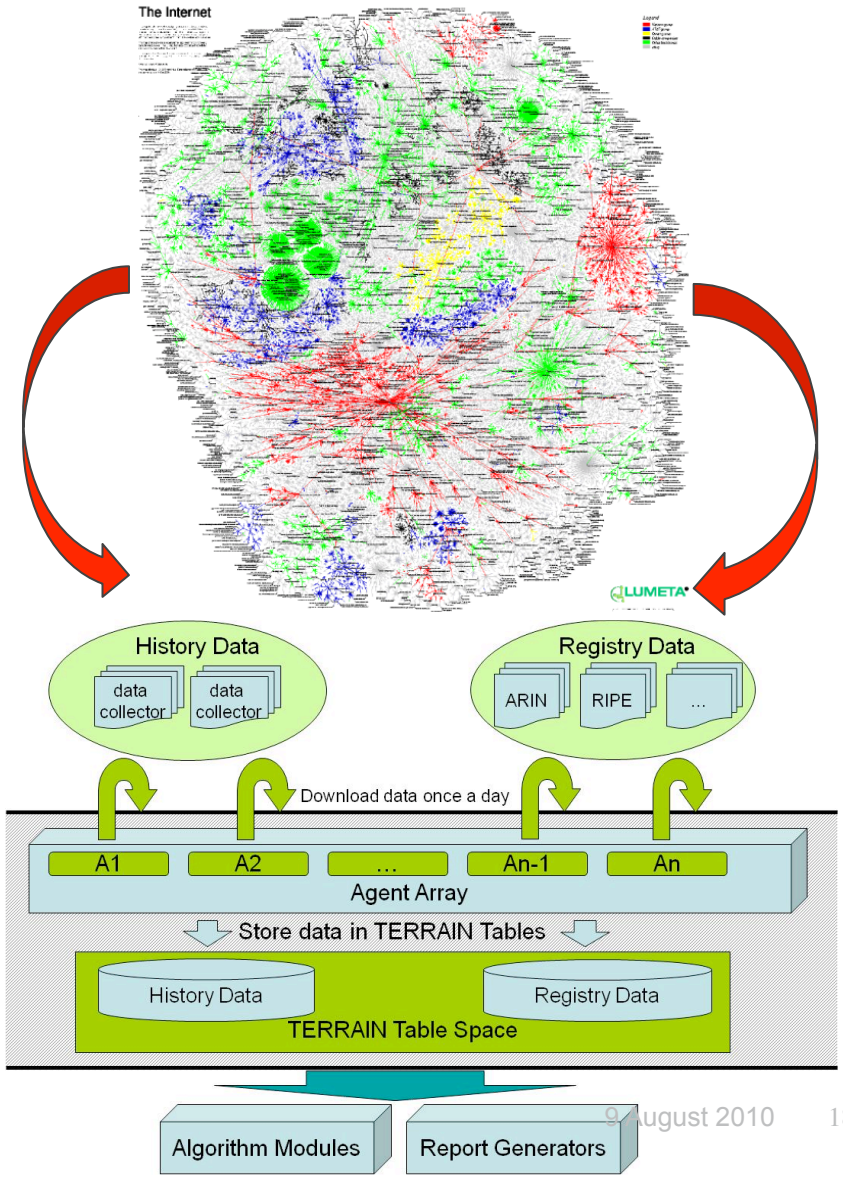
(Bogon lists, etc)



Homeland Security

TERRAIN Evaluation Framework

- **TERRAIN**
  - Continuously extracts Internet's registry and BGP monitoring data.
  - Unified data model for storing disparate data sources.
    - Designed for 5+ Terabytes.
  - Research platform for the design and analysis of robustness mechanisms.
  - Information quality measurements of registry data.
- **Historical Analysis**
  - Can present view of "BGPs world" at any point in time
  - Allows analysis over time.



Impact of TERRAIN Project

- Evaluate feasibility and commercial viability of the data driven approaches to improving BGP robustness
  - Enhance attack/anomaly detection algorithms based on combination of registry and history data
  - Evaluate corresponding anomaly response mechanisms
  - Assist the ISP industry in understanding the cost / benefit of deploying such mechanisms
- Measure and report quality of Internet registry data
  - Encourage/assist registries to improve the completeness and correctness of data
- Contribute quantitative analysis results to the design of next generation routing architectures
  - Leverage the TERRAIN experimental framework, to model and analyze new scalable routing architectures and algorithms

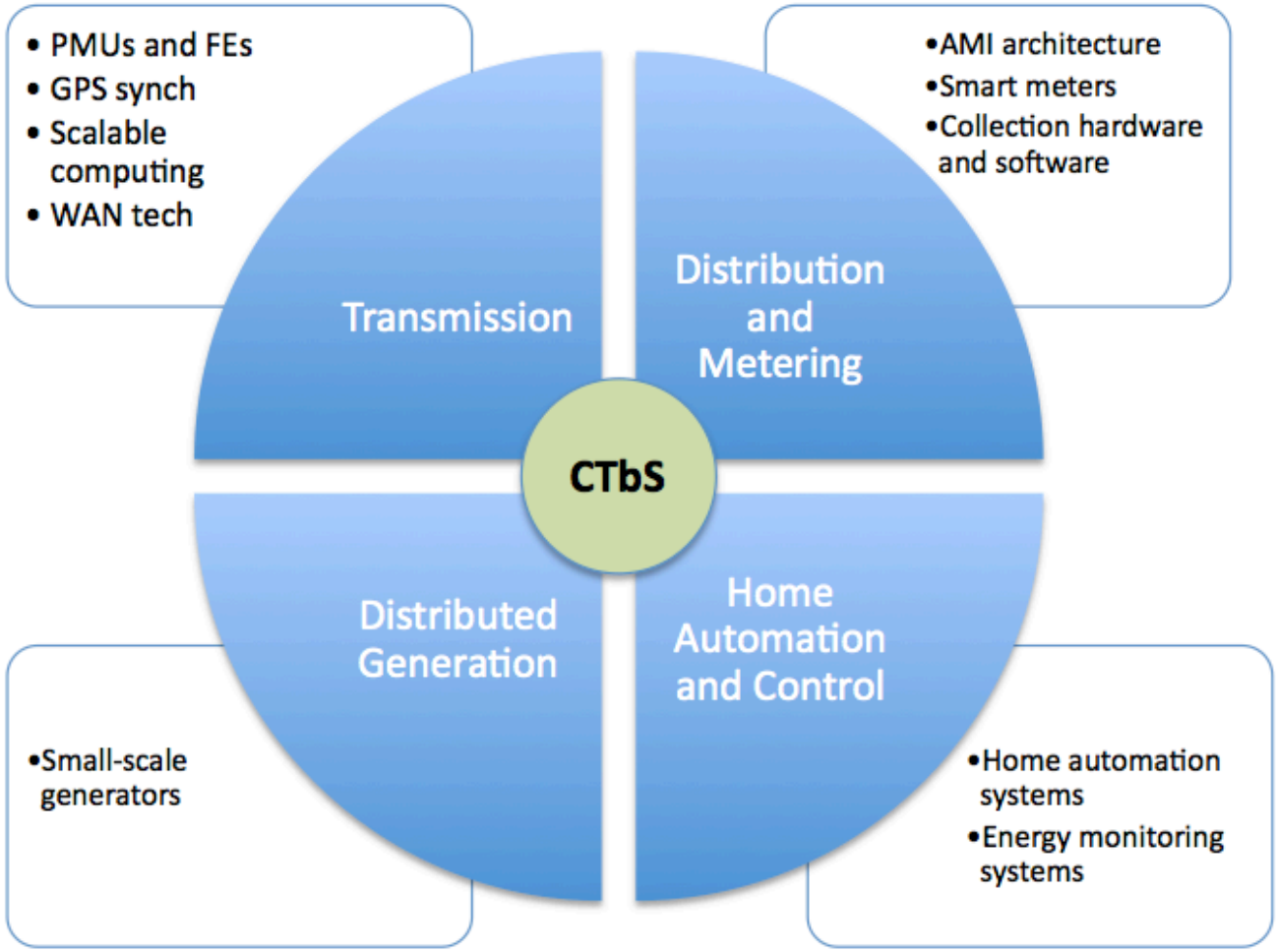
Homeland Security

TCIPG – Trustworthy Computing Infrastructure for the Power Grid

- Drive the design of an adaptive, resilient, and trustworthy cyber infrastructure for transmission & distribution of electric power
  - Protecting the cyber infrastructure
  - Making use of information to detect and respond to attacks
- Support the provisioning of a new resilient "smart" power grid that
  - Enables advanced energy applications
    - High-speed monitoring and asset control, advanced metering, diagnostics & maintenance
- Advisory Board of 30+ private sector companies

Homeland Security

Logical Organization of TCIPG Testbed



CTbS: Core Testbed Services

Ongoing Testbed Enhancements

- **Core testbed capabilities**
  - Automation and support for experiments
  - WAN integration in a contained environment
  - Virtualized core platform
- **Power System Specific experimentation capabilities**
  - Power system applications specific data generation
  - Scenario driven system configuration
  - Fault injection
  - Smart grid architecture validation
  - Proprietary hardware emulation and reconfiguration
  - Coupled system semantics
  - Full power monitoring
  - Data integration from external entities (PMU data, etc)

DARPA DDOS Study

- **"Justification and Requirements for a National DDOS Defense Technology Evaluation Facility", July 2002**
- The study envisioned a National DDoS Defense Technology Evaluation Facility whose charter would be to provide a shared laboratory in which researchers, developers, and operators from government, industry, and academia can experiment with potential DDoS defense technologies under realistic conditions, with the aim of accelerating research, development, and deployment of effective DDoS defenses for the nation's computer networks. This facility would be a shared national asset, serving a wide range of clients attacking the DDoS problem.

DARPA DDOS Study - 2

- The following requirements were identified:
  - The facility must **realistically emulate** conditions on the Internet. It must use hardware and software currently in use on the Internet, **on a scale that partially represents the Internet's complex interactions**.
  - The network must be **flexible and easily reconfigurable** so that it can support experiments requiring wide variations in network topology and hardware configuration.
  - The network must **not be a production network**. Network outages that would be unacceptable on a production network should be expected as a normal result of experimentation.
  - The environment must **provide realistic network traffic**. One of the important criteria used in evaluating DDoS defense solutions is the ability of the solution to suppress attacks while allowing legitimate traffic to flow unimpeded.
  - The environment must be **sufficiently controllable to support repeatable experiments**.
  - All proposed uses of the facility must be reviewed to ensure consistent application of the facility's charter and usage priorities.
  - The facility must have **skilled, on-site technical staff** that can help clients make efficient use of their time in the facility.
  - **Other requirements concern physical location, security, operational requirements, service level agreements, data archiving, scheduling, staffing, and funding.**

Homeland Security

DETER/EMIST Origins - 2003

Experimental Infrastructure Network (EIN) Program Solicitation
NSF 03-539

Cyber Defense Technology Experimental Research (DETER)

Networking Research Testbeds (NRT) program
NSF 03-538

Evaluation Methods for Internet Security Technology (EMIST)

Homeland Security

DETER/EMIST Vision

- Facilitate national-scale experimentation on research and advanced development of security technologies

- Approach
  - Network and computing infrastructure
  - Tools to support large-scale experimentation
  - Develop methodologies for scientific understanding of networked system security

National Research Infrastructure

- DETER - http://www.isi.edu/deter/
  - Researcher and vendor-neutral experimental infrastructure that is open to a wide community of users to support the development and demonstration of next-generation cyber defense technologies
  - Over 170 users from 14 countries (and growing)
- PREDICT – https://www.predict.org
  - Repository of network data for use by the U.S.- based cyber security research community
  - Privacy Impact Assessment (PIA) completed
  - Over 118 datasets and growing; Over 100 active users (and growing)

End Goal: Improve the quality of defensive cyber security technologies

DETER User Location Map

Vers: 4.160 Build: 01/21/2009

Tue Feb 03 1:54am PST

1057 users at 202 locations, 12 countries

DETER User Organizations

Government

- Air Force Research Laboratory
- Lawrence Berkeley National Lab
- Naval Postgraduate School
- Sandia National Laboratories
- USAR Information Operations Command

Industry

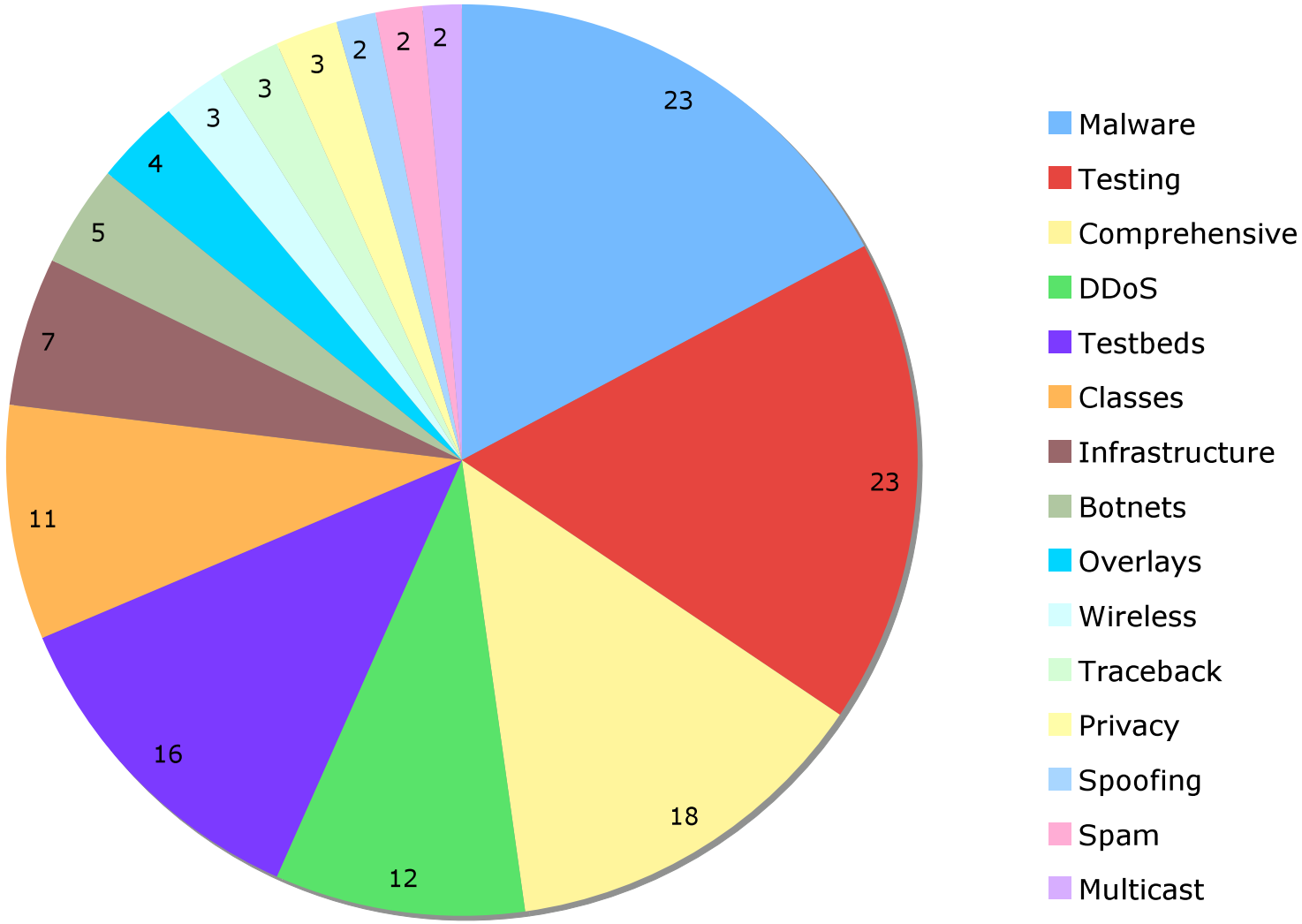
- Agnik, LLC
- Aerospace Corporation
- Backbone Security
- BAE Systems, Inc.
- BBN
- Bell Labs
- Cs3 Inc.
- Distributed Infinity Inc.
- EADS Innovation Works
- FreeBSD Foundation
- iCAST
- Institute for Information Industry
- Intel Research Berkeley
- IntruGuard Devices, Inc.
- Purple Streak
- Secure64 Software Corp
- Skaion Corporation
- SPARTA
- SRI International
- Telcordia Technologies

Academia

- Carnegie Mellon University
- Columbia University
- Cornell University
- Dalhousie University
- DePaul University
- George Mason University
- Georgia State University
- Hokuriku Research Center
- ICSI
- IIT Delhi
- IRTT
- ISI
- Johns Hopkins University
- Jordan University of Science & Technology
- Lehigh University
- MIT
- New Jersey Institute of Technology
- Norfolk State University
- Pennsylvania State University
- Purdue University
- Rutgers University
- Sao Paulo State University
- Southern Illinois University
- TU Berlin
- TU Darmstadt
- Texas A&M University
- UC Berkeley
- UC Davis
- UC Irvine
- UC Santa Cruz
- UCLA
- UCSD
- UIUC
- UNC Chapel Hill
- UNC Charlotte
- Universidad Michoacana de San Nicolas
- Universita di Pisa
- University of Advancing Technology
- University of Illinois, Urbana-Champaign
- University of Maryland
- University of Massachusetts
- University of Oregon
- University of Southern Callfornia
- University of Washington
- University of Wisconsin - Madison
- University of Wisconsin-Madison
- USC
- UT Arlington
- UT Austin
- UT Dallas
- Washington State University
- Washington University in St. Louis
- Western Michigan University
- Xiangnan University
- Youngstown State University

Homeland Security

DETER Research Areas



Homeland Security

DETER – Going Forward

- Advanced Scientific Instrument
  - Better experiment specification, management, execution
  - Improve user-facing software functions for experiment
- Advanced Testbed Technologies
  - Federation, Virtualization, Policy and Authorization Configuration, Dynamic WAN
- New Application Domains
  - Botnets, Wireless/MANET, Control Systems, HW/SW co-design
- User Outreach and Community Building
- Enhanced Infrastructure

Homeland Security

Challenge

- If you're NOT using DETER:
  - Tell us why not – what has to change in order for you to use the DETER testbed
  - How about other researchers that you talk to or work with – why aren't they using DETER? Help us find out why.
- If you are using DETER:
  - What are you doing to enlarge the community? Identify one researcher from your circle of "research friends" and get them on DETER.

Homeland Security

Summary

- DHS S&T continues with an aggressive cyber security research agenda
  - Working with the community to solve the cyber security problems of our current (and future) infrastructure
  - Working with academe and industry to improve research tools and datasets
    - Testbeds and research infrastructure is a “normal” government-funded activity and we don’t see it going away
  - Looking at future R&D agendas with the most impact for the nation, including education
- Need to continue strong emphasis on technology transfer and experimental deployments

Homeland Security

Douglas Maughan, Ph.D.
Branch Chief / Program Mgr.
douglas.maughan@dhs.gov
202-254-6145 / 202-360-3170

For more information, visit
http://www.cyber.st.dhs.gov

Homeland Security