Security in the Network Infrastructure - DNS, DDoS, etc.

GTER, São Paulo

December 8, 2006

Steve Crocker, steve@shinkuro.com
Russ Mundy, mundy@sparta.com

Proactive Security

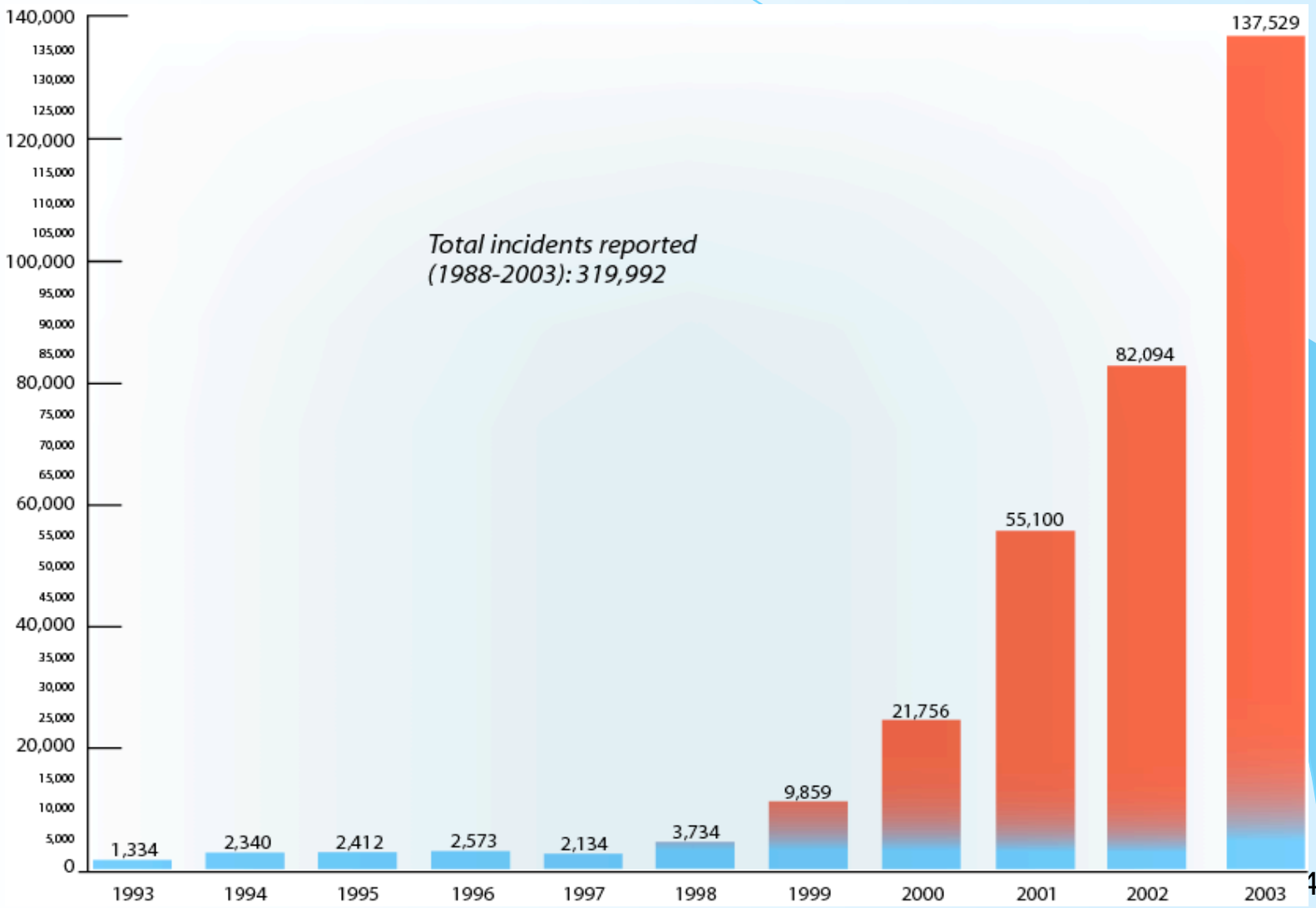
- Build security into the infrastructure
- Good architecture is cheaper and better than chasing the bad guys
  - It's less sexy but more effective

- CERTs, Firewalls, Honeynets, etc. are all good
- Networking the security community is good
- Do all of this, but also invest in the architecture

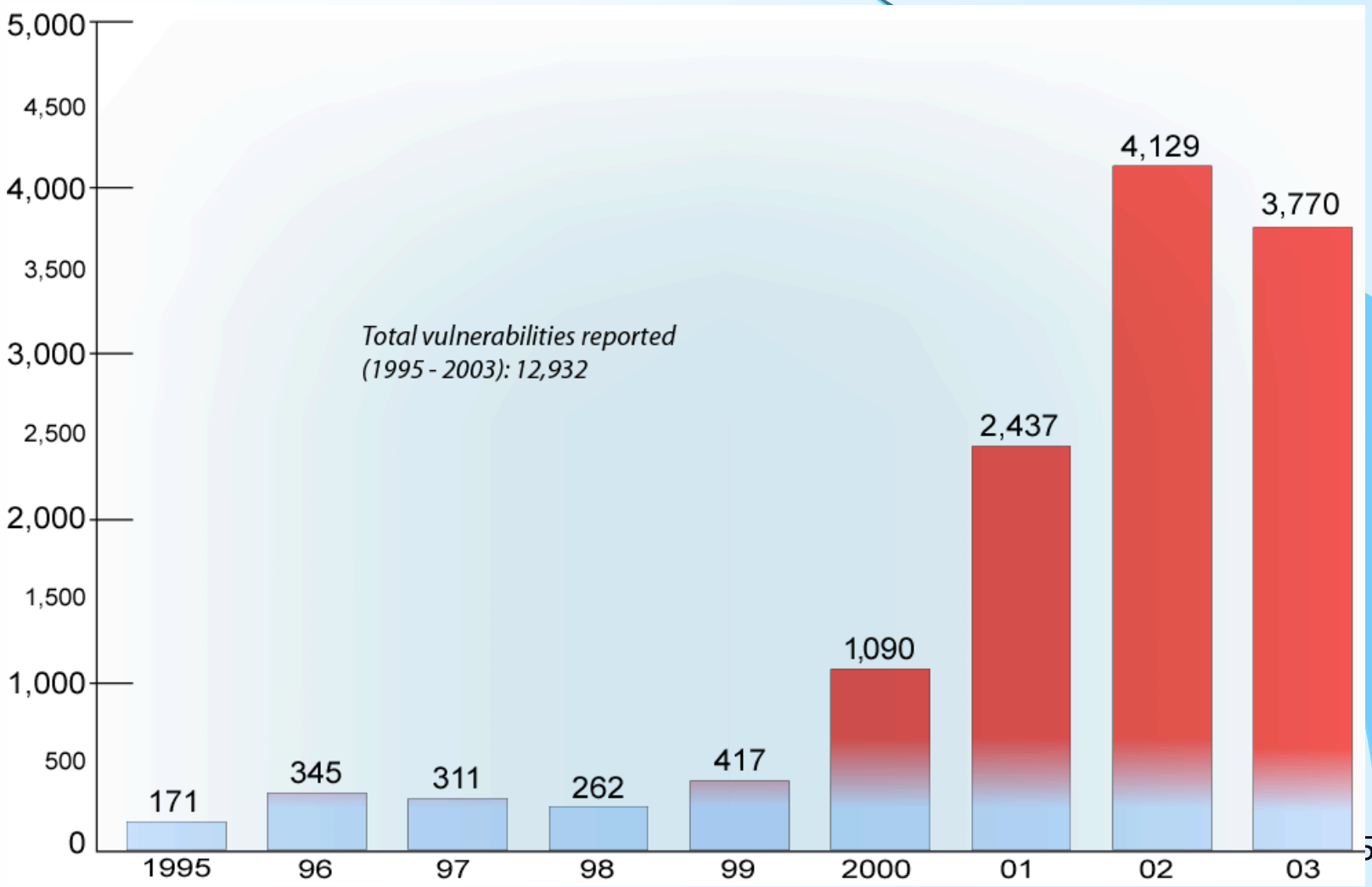
Latin America has unique opportunity

- Plenty of technical talent
- Networks are still in a growth stage
- Not as much legacy as North America, Europe
- Good communication, cooperation
- Opportunity to leap ahead

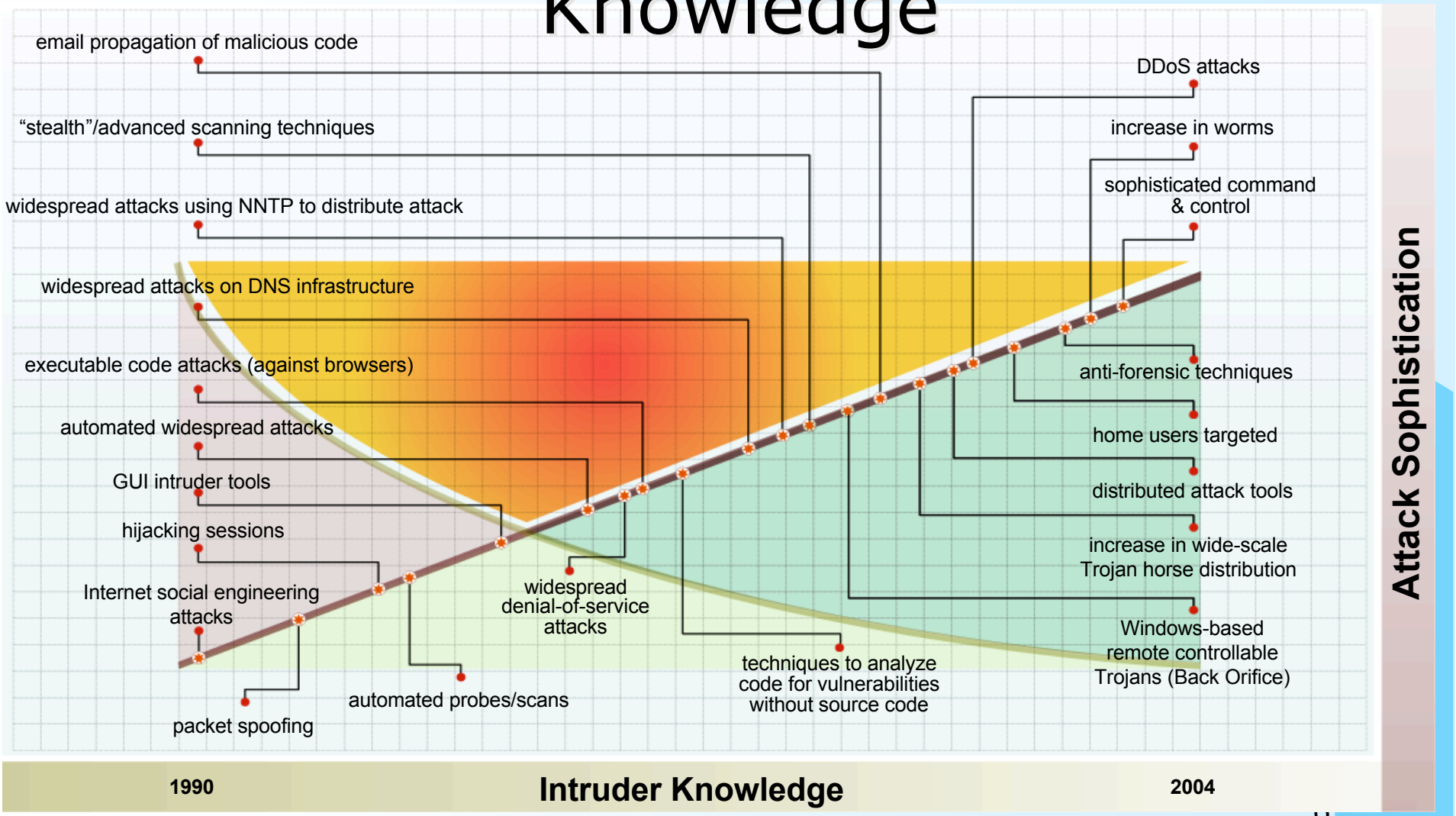
Incidents Reported to CERT/CC



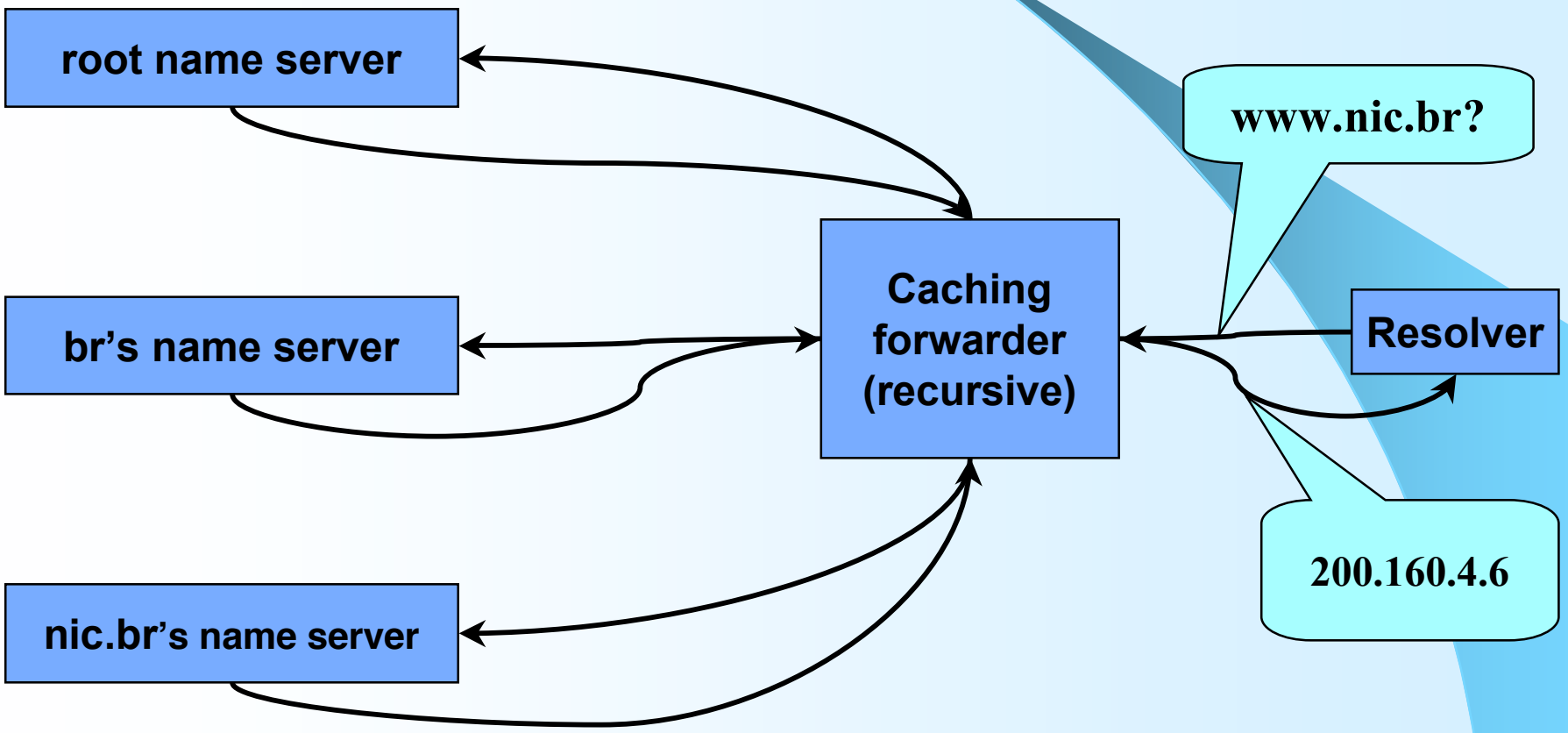
Vulnerabilities Reported to CERT/CC



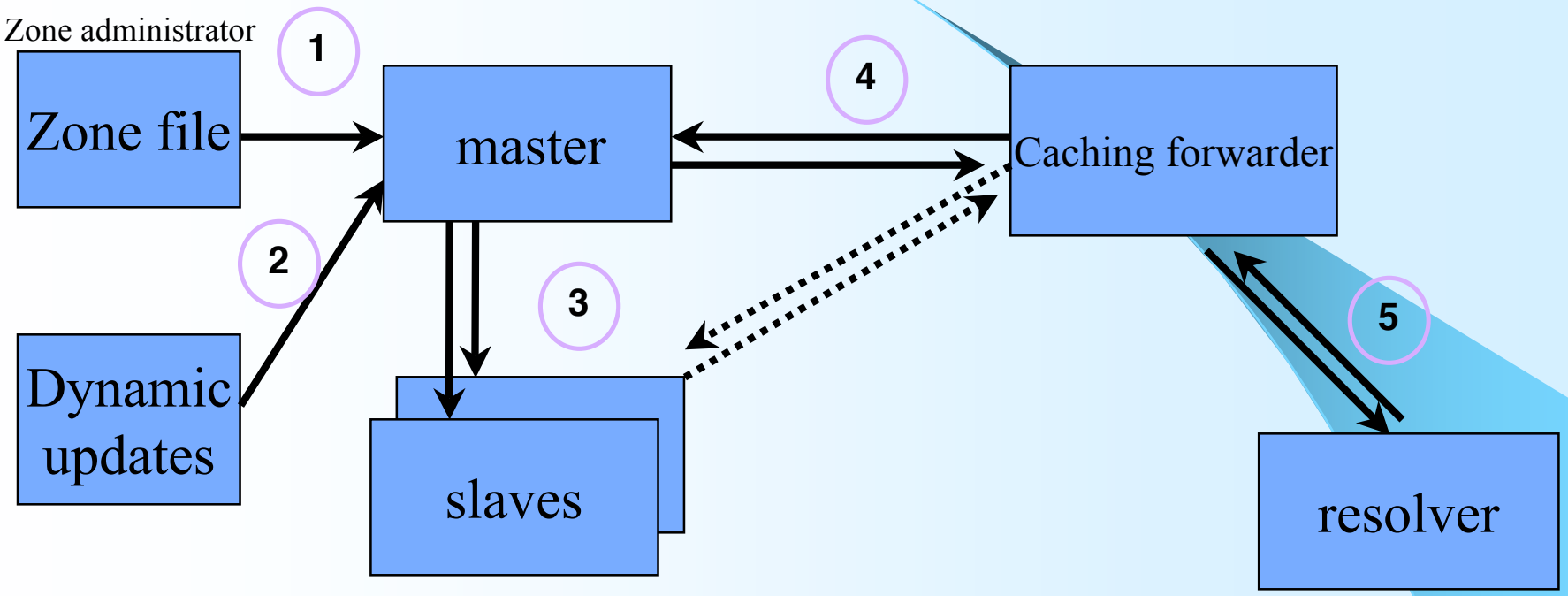
Attack Sophistication vs. Intruder Knowledge



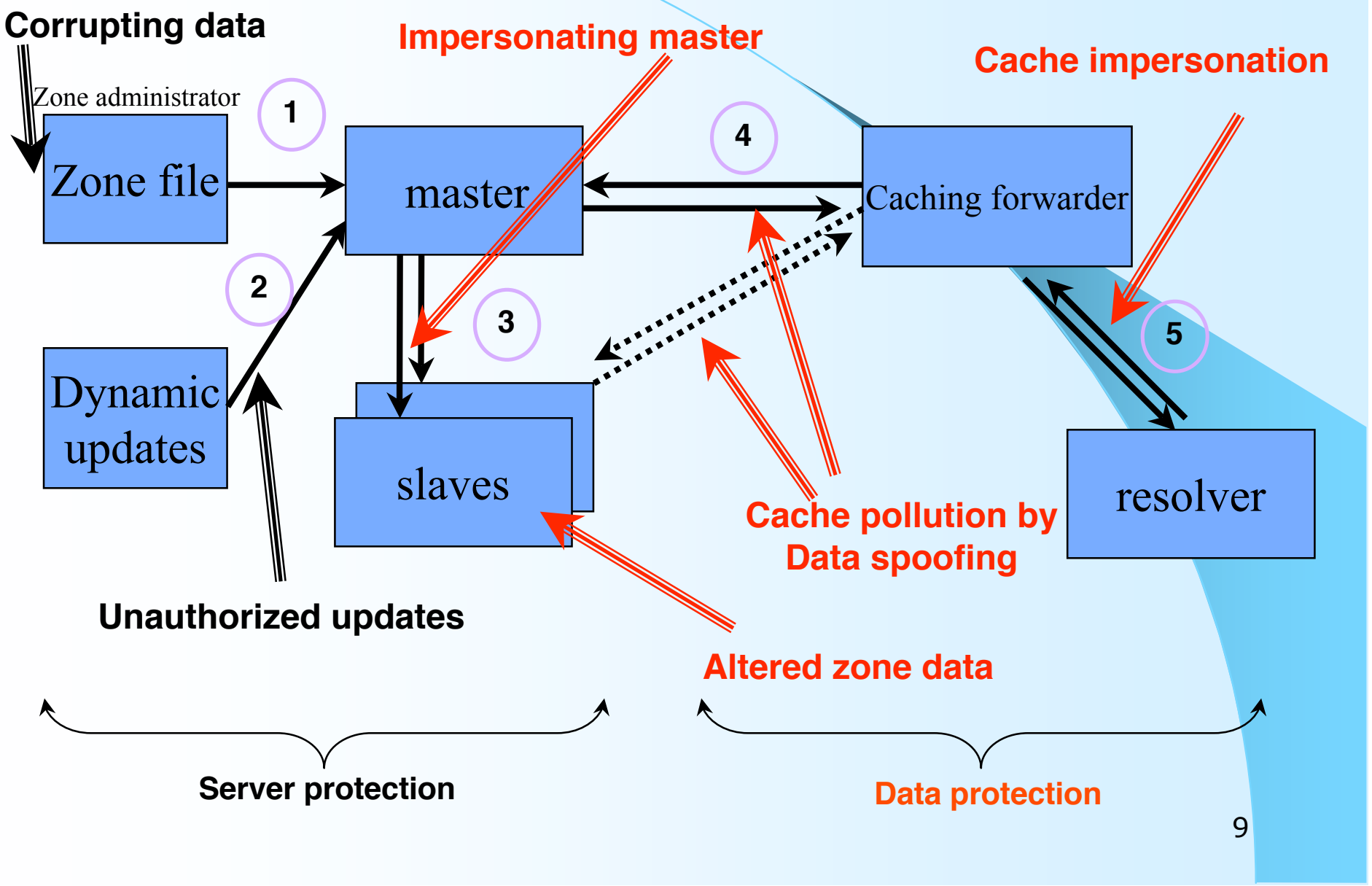
What is www.nic.br's address?



DNS: Data Flow



DNS Vulnerabilities



Securing DNS

- DNS is critical to Internet infrastructure
- DNSSEC secures DNS responses
- Specs and software are available
- Deployment has started

Hijacking Demo

Russ Mundy
SPARTA, Inc.

DNSSEC

- DNSSEC is official security protocol
  - IETF RFCs 4033, 4034, 4035
- Protects against data spoofing and corruption
- Uses public key cryptography
  - Same cryptography as PKI, but just for hosts
- Implemented hierarchically
  - The root signs the top level domain (.br)
  - The TLD signs the next level (nic.br)
  - Etc.

Deployment Status

- Specs and Software exist
- TLD deployment has begun
  - Sweden (.SE) is operational
  - Puerto Rico (.PR) is operational
  - RIPE's portion of in-addr.arpa is signed
  - .ORG, .COM and .NET have test beds
  - Others are in progress (.BR, et al)
- Browser and desktop will take a while
  - Microsoft has announced support

Getting Enterprises Signed

- In house operation
- Outsourced operation

In House Operation

- Software
- Possible hardware
- Operations Policies
  - Key lifetimes, management chain
- Procedures, Training

Outsourced Operation

- Many enterprises outsource DNS service
- Registrars, hosting services, ISPs
- Managed DNS Service Providers
  - UltraDNS, VeriSign, Akamai, Netriplex, Infoblox, EasyDNS, DNS Made Easy
- DNS Service Providers can add DNSSEC with zero imposition on domain name holder
  - Except perhaps for a charge
- **DNS Service Providers will be the source of many signed zones**

Business Opportunity

- DNSSEC fits with DKIM
  - Provides complete security picture
- Offer managed DNS service
  - High availability
  - Organized management
- Include DNSSEC service
  - Relieves burden from customer

DNSSEC Deployment

- Serious deployment activities emerging around the world:
  - http://secspider.cs.ucla.edu/ tracking ~300 signed zones
  - Europe/RIPE region most active
- U.S. Government implementing DNSSEC in its own operations
  - DNSSEC requirements included in latest Federal Information Security Management Act (FISMA) requirements
    - Federal Information Processing Standards (FIPS) 199 & 200.
  - Requires incremental deployment of DNSSEC across USG agencies ….
  - …. and the contractors that provide IT resources/services to them

Implementation Assistance

- NIST Secure DNS Deployment Guide (NIST SP800-81)
  - http://csrc.nist.gov/publications/nistpubs/
  - Provides DNS threat awareness and a range of mitigation techniques
  - Helps agencies deploy new DNS security measures with confidence
- DNSSEC Deployment Initiative
  - Growing community of organizations committed to fostering DNSSEC deployment
  - http://www.dnssec-deployment.org/
  - Resources: News, tools, deployment, test and management plans, testbeds, lessons learned
  - Free newsletter at http://www.dnssec-deployment.org/news/dnssecthismonth/

For more information,
read DNSSEC THIS MONTH
http://www.dnssec-deployment.org/
news/dnssecthismonth/

DNSSEC This Month

MAY 1, 2006 VOLUME 1, NUMBER 1

Welcome to the first edition of DNSSEC This Month, a monthly newsletter about advances in securing the Internet's naming infrastructure in the government, business and education sectors. Some 10 percent of servers in the network today are vulnerable to domain name system (DNS) attacks, and many experts expect a serious attack on the underlying infrastructure within the next decade. The DNS Security Extensions (DNSSEC) Deployment Coordination Initiative,

White House unveils R&D plan to boost IT infrastructure security: A new *Federal Plan for Cyber Security and Information Assurance Research and Development* has been issued by the White House Office of Science and Technology Policy, providing "a blueprint for coordination of Federal R&D across agencies that will maximize the impact of investments in this key area of the national interest," according to John H. Marburger III, Science Adviser to the President. The plan, available in a preprint here (http://www.nitrd.gov/pubs/csia/FederalPlan_CSIA_RnD.pdf), notes the expanding role of the domain name system, and with it, "an increased need to assure the authenticity of the DNS responses and an increased possibility that the DNS itself will be targeted for attacks." Public comments on the report were taken during April; to order a print copy of the report, click: (http://www.nitrd.gov/pubs/request.php).

DNS Security Extensions (DNSSEC) on path to be included in new federal standards: DNSSEC has been proposed as part of a new standard that aims to help federal agencies improve their information technology security and comply with the Federal Information Security Management Act (FISMA) of 2002. A plan for staged deployment of DNSSEC technology within federal IT systems was included in recently released Draft Special Publication 800-53, Revision 1: Recommended

Contacts & Resources

- Steve@shinkuro.com
- www.dnssec-deployment.org
- Slides and other DNSSEC material at: www.ripe.net/training/dnssec/
- http://www.nlnetlabs.nl/dnssec/
- http://www.dnssec.net/

Support provided by U.S. Dept. of Homeland Security, Science and Technology Directorate and ICANN

Cooperative work with SPARTA, NIST, MIT Lincoln Laboratory