SSAC
ICANN Security and Stability Advisory Committee

Public Forum

Wellington, New Zealand
March 30, 2006

Steve Crocker
steve@shinkuro.com

SSAC
ICANN Security and Stability Advisory Committee

Agenda

- **SSAC Introduction**
- Reports this week
  - Alternative TLD Name Systems and Roots
  - Amplified DNS (DDOS) Attacks
  - DNSSEC Workshop
- Upcoming work - tentative
  - Charter review
  - WHOIS comment
  - Disposition of deleted names

SSAC
ICANN Security and Stability Advisory Committee

SSAC Members

- Alain Aina
- Jaap Akkerhuis
- KC Claffy
- Steve Crocker, chair
- Johan Ihren
- Rodney Joffe
- Mark Kosters
- Allison Mankin
- Ram Mohan
- Russ Mundy
- Frederico Neves
- Jon Peterson
- Ray Plzak, vice chair
- Mike St. Johns
- Doron Shikmoni
- Bruce Tonkin
- Paul A Vixie
- Suzanne Woolf

SSAC
ICANN Security and Stability Advisory Committee

Others

- Dave Piscitello - ICANN Fellow
- Jim Galvin - Exec
- Daniel Karrenberg - Invited Guest
- Stefano Trumpy - GAC Liaison
- Patrik Fältström - IAB Liaison

SSAC
ICANN Security and Stability Advisory Committee

SSAC Role

- Security and stability expertise
- Advice to board, staff, supporting organizations, and community at large

- Advice only -- no formal authority

SSAC
ICANN Security and Stability Advisory Committee

SSAC Reports

- Usually related to specific incident/issue
  - Findings, Recommendations
- Opportunity for explanation of an area
  - Useful beyond specific incident/issue
- Broad sense of security and stability
  - Protection of registrants, users, end-systems

SSAC
ICANN Security and Stability Advisory Committee

Agenda

- SSAC Introduction
- **Reports this week**
  - **Alternative TLD Name Systems and Roots**
  - **Amplified DNS (DDOS) Attacks**
  - **DNSSEC Workshop**
- Upcoming work - tentative
  - Charter review
  - WHOIS comment
  - Disposition of deleted names

SSAC
ICANN Security and Stability Advisory Committee

DNSSEC Deployment

- DNSSEC is coming
- .SE and RIPE's portion of in-addr.arpa are signed
- More coming -- .ORG

- DNS Service Providers will be the path for large numbers of signed zones

SSAC
ICANN Security and Stability Advisory Committee

Agenda

- SSAC Introduction
- Reports this week
  - Alternative TLD Name Systems and Roots
  - Amplified DNS (DDOS) Attacks
  - DNSSEC Workshop
- **Upcoming work - tentative**
  - **Charter review**
  - **WHOIS comment**
  - **Disposition of deleted names**

SSAC
ICANN Security and Stability Advisory Committee

Alternative TLD Name System and Roots

Dave Piscitello,
on behalf of ICANN SSAC

SSAC
ICANN Security and Stability Advisory Committee

What are we talking about?

- Alternative TLD name system operators
  - Organizations that register names in TLDs outside the delegation process sanctioned by ICANN
- Alternative root service operators
  - Organizations that operate root services and resolve TLD labels outside the authoritative root
- Alternative root zone authorities
  - Organizations other than IANA that publish a root zone
- Often called alternate-roots or alt-roots

SSAC
ICANN Security and Stability Advisory Committee

Types of alternative TLD name system and root operators

- Private
- Experimental
- Commercial
- Protest
- Politically motivated

SSAC
ICANN Security and Stability Advisory Committee

Private TLD Name Systems and Root Services

- Operate within closed community
  - Intra-and inter-organizational, institutional, enterprise
- Support name schema and name service that has context within that organization
- Isolated from authoritative DNS
- No threat to single authoritative TLD name system and root name service

SSAC ICANN Security and Stability Advisory Committee

Experimental TLD Name Systems and Root Services

- Operates within closed community
- Supports a name schema and name service for research and experimentation
  - Next generation Internet Protocol test beds
  - International languages and character sets in top level domain labels
- Isolated from authoritative root
- No threat to single authoritative TLD name system and root name service

SSAC ICANN Security and Stability Advisory Committee

Commercial TLD Name Systems and Root Name Services

- Regard TLDs as a potentially lucrative business
- Consider ICANN accreditation process a business impediment and overly constraining
- Philosophies include:
  - No limits should be imposed on the creation of TLDs,
  - Approval process for operators should be as simple as creating a corporation
  - The market will decide how many TLDs are needed
  - *caveat emptor* applies

SSAC
ICANN Security and Stability Advisory Committee

Protest TLD Name Systems and Root Services

- Operate name systems that
  - Restrict membership, or
  - Filter or censor content, or
  - Embrace "Internet is free, anyone can play" attitude, or
  - Embrace activism (political, environmental, …)
- “Democratic” TLD label registration
  - Low admission criteria for membership
  - Simple voting majority enough to adopt new TLD labels

SSAC
ICANN Security and Stability Advisory Committee

Politically motivated TLD name systems and roots

- Established by sovereign nations and multi-national alliances
  - Sometimes called "breakaway" roots
- Reasons for initiatives include
  - Governance
  - Trust
  - Control
  - Reliability, availability, fair allocation of cost and resources (root server operations)
  - National and local character set support in TLD labels (“internationalized” TLDs)

SSAC
ICANN Security and Stability Advisory Committee

Issues

- Does the alternative operator
  - Resolve disputes (name ownership, IP…)?
  - Demonstrate its solvency?
  - Assure uniqueness of TLD labels?
  - Assure universal resolvability?
  - Assure availability of root name service?
  - Assure non-interference with
    - Competing operators?
    - Registries operating under agreements with ICANN?
- To whom is the alternative operator accountable?

SSAC
ICANN Security and Stability Advisory Committee

Universal service or Walled Gardens?

- Will politically motivated TLD name system deploy name services to
  - Enhance commercial and economic interest?
  - Control user behavior and access to content
  - Substitute or censor content
  - Require that ISPs use their root name servers?
- Who coordinates character sets for (g)TLDs?

SSAC
ICANN Security and Stability Advisory Committee

In practice

- Universal resolvability is lost
  - General case is that users can't resolve TLDs from authoritative DNS and multiple alternative TLD root operators
    - Reconfiguration/reboot required
    - Host files must be modified
    - Software required
- Root zone composition is typically union of authoritative root plus *one* alt-root
  - No way to coordinate and publish the über-root zone file
  - Commercial and self-interests actually discourage universal resolvability
    - Difficult to prevent duplicate TLD labels

SSAC
ICANN Security and Stability Advisory Committee

Registrant Issues

- Are registrants adversely affected when they register domain names in alternative TLDs?
  - Majority of 972M end users are not familiar with alternative TLDs
  - Majority of client software is only configured to resolve names via the authoritative root
  - If user's can't resolve your domain, are you conceding a $2T + ecommerce, B2B, tourism… to competitors whose names *are* resolvable via the authoritative root?
  - If your mobile employees cannot universally resolve your domain name, are they truly mobile?

SSAC
ICANN Security and Stability Advisory Committee

Findings (1 of 2)

- **Finding (1):** SSAC can find little evidence to support claims that commercial alternative TLD name systems have or will attract a significant market share to fragment the root.

  Alternative TLD name systems may create barriers to an estimated two trillion dollar (USD) e-commerce market and constrain business-to-business collaboration, tourism, commercial and other opportunities for registrants. Registrants who attempt to support global mobility for end users may be similarly affected.

SSAC
ICANN Security and Stability Advisory Committee

Findings (2 of 4)

- **Finding (2):** Countries that will not wait for ICANN to adopt a internationalized TLD policy and by countries that choose to follow policy directions opposite to those arrived at using the ICANN collaborative policy development process can fragment the root.

  Many political reasons exist for countries to choose this course. ICANN cannot control how countries behave, but should (continue to) work towards a technically sound solution that is best for the Internet community.

SSAC
ICANN Security and Stability Advisory Committee

Findings (3 of 4)

- **Finding (3):** At a technical level, multiple methods for supporting internationalized domain names exist. ICANN has announced a time line for the development of a project for the technical test of internationalized TLD labels.

  SSAC believes that the technical test plan is essential. Technical alternatives must be evaluated, a choice must be made, and trials must be conducted to assure that the root level of the DNS is ready for a production environment before a consensus policy might be reached.

SSAC
ICANN Security and Stability Advisory Committee

Findings (4 of 4)

- **Finding (4):** ICANN will find it necessary to increase the number of TLDs to accommodate internationalized TLD labels and continued commercial interest. The root name server operations can accommodate a substantial increase in the size of the root zone.

  However, the technical aspects of name service are but one factor to consider. ICANN must review the existing TLD approval process as well as the processes whereby TLDs are introduced into the root zone (for subsequent ongoing administration) to ensure that all operations associated with adding TLDs can support the increase in TLDs.

SSAC
ICANN Security and Stability Advisory Committee

Recommendations

- **Recommendation (1):** ICANN and the community at large should take appropriate measures to ensure that a thorough analysis of two candidate methods for encoding strings in TLD labels - DNAME Equivalence Mappings and use of IDNA encodings – is concluded quickly. Based on the conclusions and recommendations of parties responsible for this analysis, ICANN should adopt the preferred method.

- **Recommendation (2):** ccTLD registries should actively participate in the ICANN IDN Experimental Testbed projects and provide their perspectives on the implementation of “internationalized” TLD labels in the root. SSAC recommends that ccTLD registries and national or regional linguistic organizations not implement standalone or alternate TLD schemes until the results of the IDN Experimental Testbed are evident.

SSAC
ICANN Security and Stability Advisory Committee

Amplified DNS Distributed Denial of Service (DDOS) Attacks

Wellington, New Zealand
March 28, 2006

Rodney Joffe rjoffe@ultradns.net
Dave Piscitello
dave.piscitello@icann.org

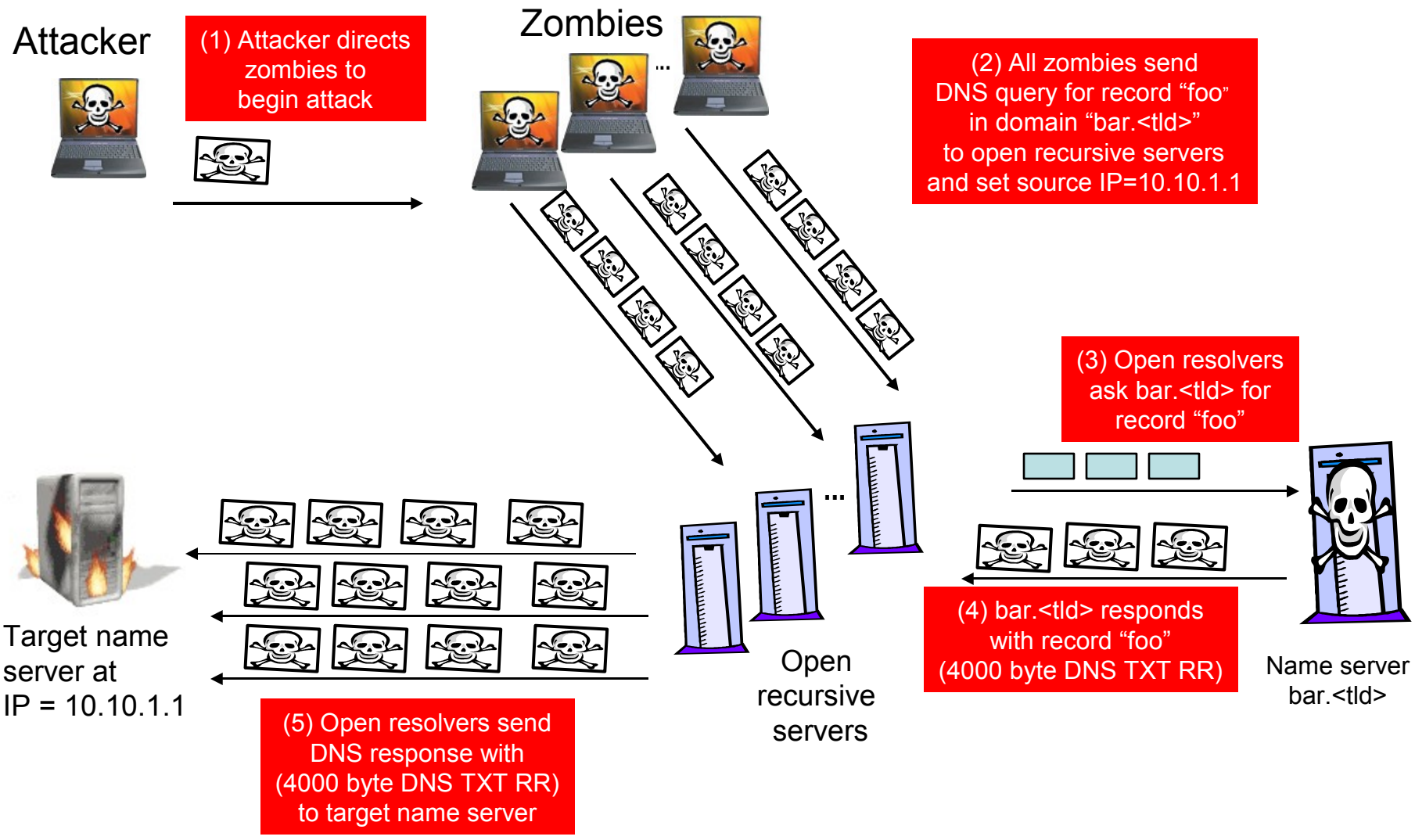
SSAC
ICANN Security and Stability Advisory Committee

Background

- January - February, 2006
  - Authoritative TLD DNS servers attacked
  - Variant of a well-known DDoS attack
  - Exploited 500,000+ innocent but vulnerable recursive servers
  - Attacks generated from 2 - 8 Gbps of traffic at targeted Authoritative DNS Servers
  - Failures occurred in networks in the path as well as transit providers to the authoritative TLD DNS servers
  - Resulted in disruption of DNS services in every case
  - Included many TLDs without any apparent motive in most cases

SSAC
ICANN Security and Stability Advisory Committee

Anatomy of the Attack



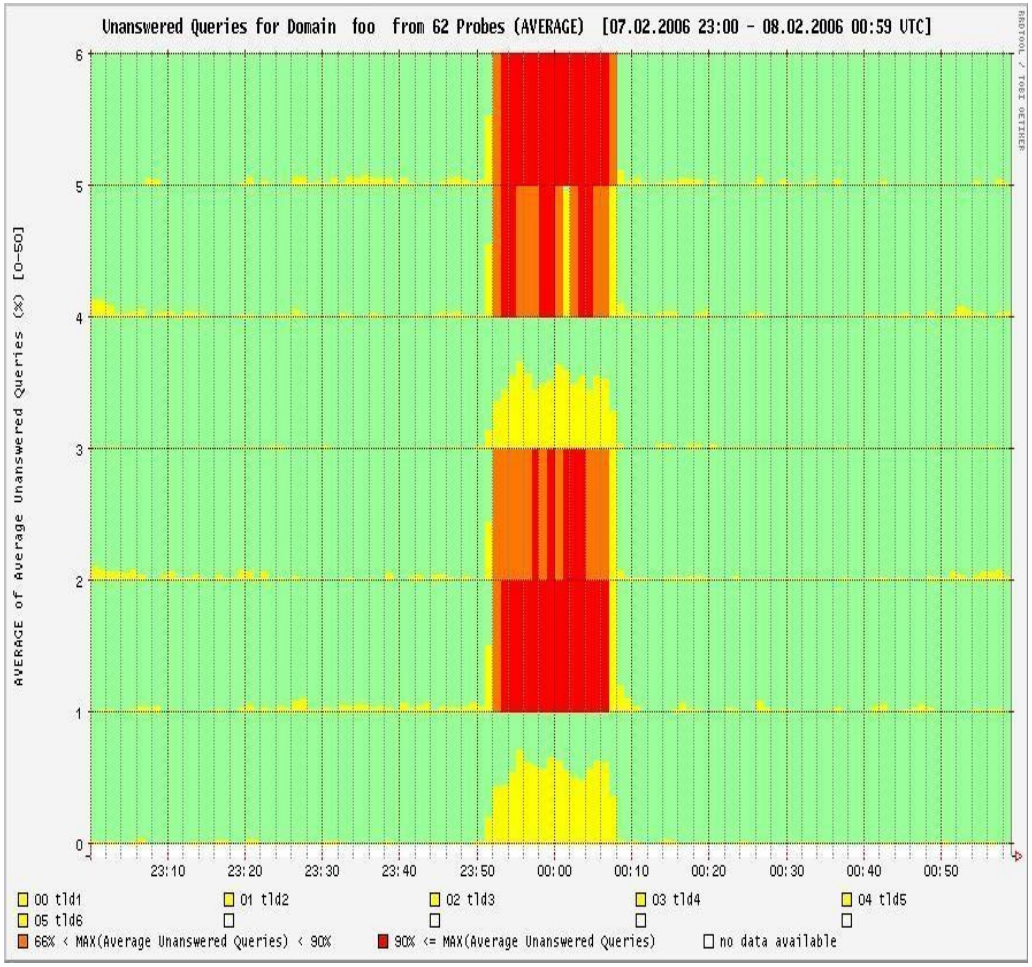
SSAC
ICANN Security and Stability Advisory Committee

Detailed analysis of one attack

Graph of responses to monitoring probes by the authoritative nameservers for a TLD before, during, and after an attack in February 2005.

Vertical Axis shows the six TLD Server IP addresses. Red shows complete failure to answer, yellow indicates slow answers. For reference, Servers 1 and 4 show lesser impact than Servers 2, 3, 5, and 6. The horizontal axis shows actual time. This attack lasted 14 minutes.

Graphs courtesy of RIPE NCC.



SSAC
ICANN Security and Stability Advisory Committee

Attack Metrics:

- 51,000 open recursive servers were involved
- 55 byte query resulted in a 4,200 byte response, for a 1:76 amplification
- 8gbps attack requires a total of 108mbps of queries.
- Each recursive server saw 2,100 bytes of queries, or 38 qps, and responded with 160kbps in answers
- Assuming compromised hosts have minimum 512kb DSL modem, only 200 compromised hosts were required
- Source networks would see no effect
- Recursive servers saw minimal traffic or query increase
- Victim network providers had catastrophic experience
- Victim DNS provider was sent the equivalent of 150 million qps
- At best, 1 in 100 real queries were answered

SSAC
ICANN Security and Stability Advisory Committee

Enabling Vectors

- The following specific vectors that allowed the Reflective Recursive DNS DDoS attacks against the Authoritative TLD DNS servers have been identified by the ICANN SSAC:

- Network Providers (ISPs)
  - Failure to prohibit forging or spoofing of IP addresses by hosts
  - Failure to prohibit traffic from IP addresses they are not authorized to originate from exiting their networks

- Recursive Server Operators
  - Accepting and responding to DNS queries from IP addresses not under their control
  - Running nameserver versions with known vulnerabilities that allow destructive records to be configured by unauthorized parties

SSAC
ICANN Security and Stability Advisory Committee

Countermeasures

- Source IP validation
- Disable open recursive service
- Securely configure DNS Servers
- Implement blocking and filtering

SSAC
ICANN Security and Stability Advisory Committee

Recommendations (1 of 3)

- Recommendation (1): For the long term, SSAC recommends that the most effective means of mitigating the effects of this and numerous DoS attacks is to adopt source IP address verification.

SSAC
ICANN Security and Stability Advisory Committee

Recommendations (2 of 3)

- Recommendation (2): SSAC specifically recommends that each ROOT and TLD name server operator should:
  - Document operational policies relating to countermeasures it will implement to protect its name server infrastructure against attacks that threaten its ability to offer service, give notice when such measures are implemented, and identify the actions affected parties must take to have the measures terminated.
  - Respond faithfully and without undue delay to all questions and complaints about unanswered traffic, and
  - Act with haste to restore service to any blocked IP address if the owner of that IP address can demonstrate that it has secured its infrastructure against the attack.

SSAC
ICANN Security and Stability Advisory Committee

Recommendations (3 of 3)

- **Recommendation (3):** SSAC recommends that name server operators and Internet Service Providers consider the possible remedies described in Section 3 of this Advisory.

  In particular, SSAC urges name server operators and ISPs to *disable open recursion* on name servers from external sources and only accept DNS queries from trusted sources to assist in reducing amplification vectors for DNS DDoS attacks.