ICANN and Internet Security

Steven M. Bellovin
AT&T Labs — Research
smb@research.att.com
http://www.research.att.com

Why Are We Here?

- To decide if there's a problem for ICANN to solve.
- To understand what problems belong to someone else.
- To decide how to move forward.

What is ICANN?

- ICANN is "the non-profit corporation that was formed to assume responsibility for the IP address space allocation, protocol parameter assignment, domain name system management, and root server system management functions".
- ICANN *does not* define protocols.
- ICANN *does not* operate the Internet.
- ICANN *is not* the governing body for the net.

Implications

- ICANN cannot solve "the" whole Internet security problem — and it shouldn't try to.
- It can — and should — promote protection of the name and number services upon which the Internet relies.
- That might best be accomplished by asking some other organization to do some things.
- ICANN must get buy-in from others.

Areas of Concern

- Address allocation
- Domain name system management
- Root name server management

Address Allocation

- Who owns addresses?
  - The database is very dirty, especially for older addresses.
  - Sub-allocations often not recorded.
- Cannot secure routing without authoritative ownership information.
- Only implementable by address registries and ISPs.
- How can ICANN facilitate this?

Root Name Server Management

- Many issues!
  - Host security
  - Availability
  - Routing
  - Lack of diverse implementations
- ICANN cannot mandate solutions:
  - ISPs control routing.
  - Root server operators control host software.
  - Quirks of DNS protocol definition may interfere.
  - Etc.
- Must negotiate best solution.

Domain Name System Management

- The fun part...
- Many different components.
- Bad guys don't go through security; they go around it.
- *Must secure total system!*

Major Components

- Name Servers
- Resolvers
- Registry (and its databases and software)
- Registrars (and their databases and software)
- Customers (and their software)
- Registry-registrar protocol
- Customer-registrar protocol(s)
- Back-end protocols and software.

Software

- ICANN cannot — and should not — dictate what operating systems or protocol implementations are to be used.
  - Too many choices, too many issues, too much religion, too little ability (for anyone?) to promulgate reasonable standards.
- But — most security problems are due to buggy code.

Protocols

- ICANN doesn't define protocols.
  - The IETF defines the DNS protocols.
- But it can give its requirements to a group that does.
- What are those requirements? For which protocols?
  - Integrity? Confidentiality? Authentication? Availability?
  - DNSSEC? Registry-to-registrar? Others?

Registrars

- Who is responsible for registrar security?
- ICANN?
  - How?
  - Who is liable for failures?
- Let the market decide?
  - What happens to customers who, due to a security failure, cannot prove domain name ownership?
  - Digitally signed, timestamped receipts?

Registries

- Regulated "monopolies" -- can't let market decide.
- What is "good enough"?
- How are standards set? Audited?
- Who is liable for failures?
- What disaster recovery mechanisms should be used?

Customers

- How strong must the customer-registrar authentication be?
- Who is responsible for forged change requests?
  - There have been many incidents of such forgeries.
- Who *really* owns a domain name registered by a hosting company? Is ICANN involved?
- Who is responsible for fall-back authentication for lost keys, forgotten passwords, etc.?

Conclusions

- Yes, there is a real problem that ICANN should address.
  - ICANN is only responsible for a small piece of the total problem.
- Even within ICANN's space, ICANN cannot solve its problems alone.
- The hard part — and the part for ICANN to do — is to set the requirements.
- But even that can't be done in a vacuum.