

DSSA Update

Costa Rica – March, 2012



Goals for today

- Update you on our progress
- Raise awareness
- Solicit your input



Charter: Goals and Objectives

Report to participating SO's and AC's on:

- Actual level, frequency and severity of **threats to the DNS**
- Current efforts and activities to mitigate these
- Gaps in the current response to DNS issues
- Possible additional risk mitigation activities that would assist in closing those gaps



Unpacking some terms

Our charter speaks to “Threats”

Threat-events (what happens) should not be confused with:

- **Adverse impacts** - that may result
- **Vulnerabilities** - that allow them to happen
- **Predisposing conditions** - that influence adverse impact once they’re under way
- **Controls and mitigation** – that reduce likelihood and impact
- **Threat-sources** – which exploit vulnerabilities to initiate them



Activity since Dakar

- The working group has:
 - Developed a **protocol for handling confidential information**
 - Selected, and begun to tailor, a **methodology** to structure the remaining work
 - Begun the **detailed analysis** of the risk assessment



Methodology – NIST 800-30

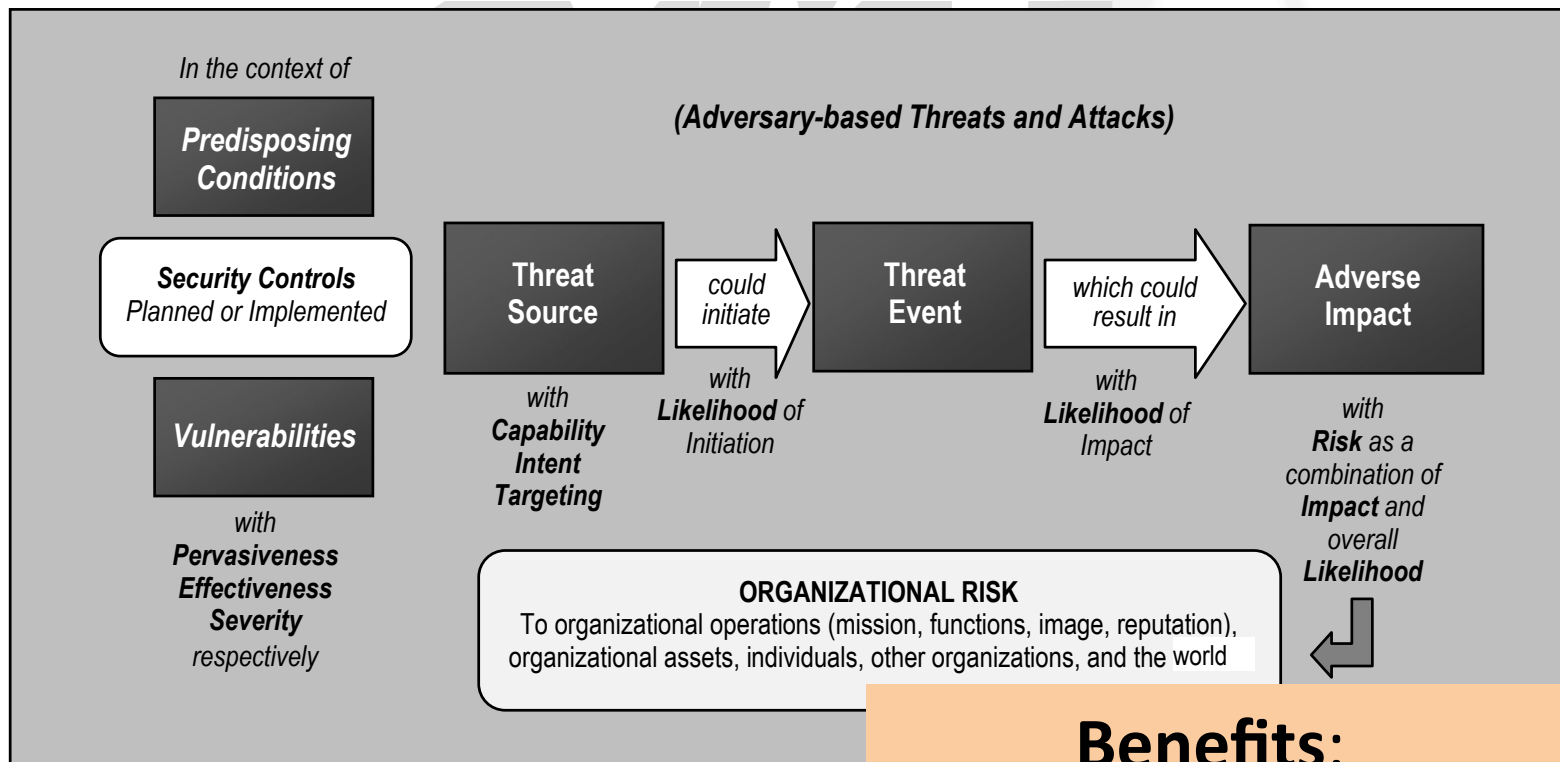
Rationale

- Using a predefined methodology will save time and improve our work product
- Reviewed several dozen alternatives
- We selected this one because it's:
 - Available at no cost
 - Actively supported and maintained
 - Widely known and endorsed in the community
 - Reusable elsewhere in ICANN



Methodology – NIST 800-30

Example – Adversarial Risk Model



Benefits:

- Consistent terminology
- Shared model
- Structured work
- Sample deliverables



Where we are...

Approach

Launch

Identify Threats &
Vulnerabilities

Analyze
Threats & Vulnerabilities

Report

We are here – getting started
with this phase of the work

We are hoping to have a high-level
version of this done by Prague



Where we are...

Status

- 43 weeks (or 43 hours) in
- We've developed substantial (and reusable)
 - **Data**
 - **Methods**
- Given our **resources**, pick any 2 of 3 going forward
 - **Detail** (identify vs. analyze high-risk scenarios)
 - **Speed** (6 months vs. 36)



Where we are...

Determinations – Threat events and level of impact

Level of Impact:

In the worst case there would be broad harm/consequence/impact to operations, assets, individuals, other organizations and the world if any of these threat-events occur. And in all cases there would be significant problems for registrants and users in the zone.

Threat events:

- Zone does not resolve
- Zone is incorrect
- Zone security is compromised



Where we are...

Determinations – Nature of impact

- Damage to a critical infrastructure sector
- Damage to trust relationships or reputation
- Harm to individuals
- Harm to assets
- Harm to operations



Where we are going

- **Vulnerabilities** – severe and widespread?
 - **Predisposing conditions** – pervasive?
 - **Controls and mitigation** – effective and deployed?
- **Threat sources** – how broad is range of impact, what are their capabilities, how strong is their intent, are they targeting the DNS?
 - **Initiation** – what is the likelihood that a threat-event will happen?
- Given all of the above – **what are the high-risk scenarios?**



Questions?



How we work

(design credit -- CLO)

Live chat

Participants

Polling

The screenshot shows an Adobe Connect meeting window titled "Joint DNS Security and Stability Analysis Working Group (Sharing) - Adobe Connect". The interface includes a chat window on the left, a central shared document window, and a right-hand sidebar with attendees and sharing options.

Chat (Everyone):

- Jacques Latour: we have very small deployment of DNSSEC on the planet
- Olivier Crepin-Leblond: Time?
- Olivier Crepin-Leblond: Apologies but I need to go
- Clayton Langdon-Orr: Be there soon OCL
- Olivier Crepin-Leblond: ok
- Patrick Jones: I have to drop off as well
- Joerg Schweiger: I'd reverse my vote
- Jacques Latour: next time will have audio
- Joerg Schweiger: bye folks
- bart: Bye all, see you next week
- Katrina Sataki: thank you! bye!
- Rossella Mattioli: thank you, bye!
- Mike O'Connor: Nathalie, have you grabbed the chat transcript yet?

Shared Document: A table titled "Threat sources -- range of effects" and "Threat events -- relevance".

Description	Identifier	Description	Range of effects (see "Scales" tab)	Relevance to the DNS (see "Scales" tab)
			10 8 5 3 1 Avg Dev	10 8 5 3 1 0 Avg
Configuration errors by privileged users	NATE-40	Root zone -- an individual administrator changes an operational parameter that removes the zone from being published or publishes it incorrectly	1 7 3.25	4 4 2.00
Configuration errors by privileged users	NATE-50	Root zone -- misconfigure the IANA zone file	8 2 5.00	7 1 0.88
Configuration errors by privileged users	NATE-60	"Major" DNSSEC provider (somebody who does DNS services, eg DynDNS, Neustar, large businesses, etc) -- localized to the community served by that provider.	3 1 2.00	10 1.00
Configuration errors by privileged users	NATE-70	DNSSEC for a TLD zone	5 9 7.00	1 8 2 2.82
Configuration errors by privileged users	NATE-80	Critical DNS support files (e.g., Hint, whois, servers.net -- the zone where all the servers are listed; Roots public suffix configuration files)	3 7 5.90	2 8 5.60
Configuration errors by privileged users	NATE-90	A registry administrator misconfigures provisioning systems between registries and registers the result being that registrars can't add/change/delete zones from the TLD -- EP is one way to do that, but there are others	4 6 1.80	7 1 2.75
Business failure of a key provider	NATE-10	Disrupts a "major" zone file (.COM/.NET/.UK/.DE etc.)	7 5 6.00	7 1 1.00
Business failure of a key provider	NATE-20	Disrupts a "lesser" zone file (that is not outsourced to a major provider)	6 3 4.50	10 1 9.82
Business failure of a key provider	NATE-30	Root zone -- is published incorrectly	2 3 1 8.17	6 3 3.00
Business failure of a key provider	NATE-40	Root zone -- is not published	5 1 1 9.00	6 1 0.86
Business failure of a key provider	NATE-50	Disrupts the IANA zone file	6 1 1 10.00	7 1 1.00
Business failure of a key provider	NATE-60	Disrupts DNSSEC from a "Major" DNSSEC provider	6 1 7 00	2 3 7.75
Business failure of a key provider	NATE-70	Disrupts DNSSEC for a TLD zone	6 1 7 00	1 7.75

Threat sources -- range of effects:

- 11 -- sweeping, involving almost all of the cyber resources of the DNS
- 8 -- extensive, involving most of the cyber resources of the DNS
- 5 -- wide-ranging, involving a significant portion of the cyber resources of the DNS
- 3 -- limited, involving some of the cyber resources of the DNS
- 1 -- minimal, involving few if any of the cyber resources of the DNS

Threat events -- relevance:

- 10 - Confirmed -- Seen by the organization
- 8 - Expected -- Seen by the organization's peers or partners
- 5 - Anticipated -- Reported by a trusted source
- 3 - Predicted -- Predicted by a trusted source
- 1 - Possible -- Described by a somewhat credible source
- 0 - Not applicable (check after call)

Agenda:

- DSSA Working Group 26 January 2012
- Agenda
- Roll call and update SOI's
- Approach
- Architecture
- Analysis -- Threat Sources (Tables D-7 & D-8)
- Any other business (AOB)



Definitions

Agenda

Charter: Background

At their meetings during the ICANN Brussels meeting the At-Large Advisory Committee (ALAC), the Country Code Names Supporting Organization (ccNSO), the Generic Names Supporting Organization (GNSO), the Governmental Advisory Committee (GAC), and the Number Resource Organization (NROs) acknowledged **the need for a better understanding of the security and stability of the global domain name system (DNS)**. This is considered to be of **common interest** to the participating Supporting Organisations (SOs), Advisory Committees (ACs) and others, and should be preferably **undertaken in a collaborative effort**.



Methodology – NIST 800-30

Risk Management Hierarchy

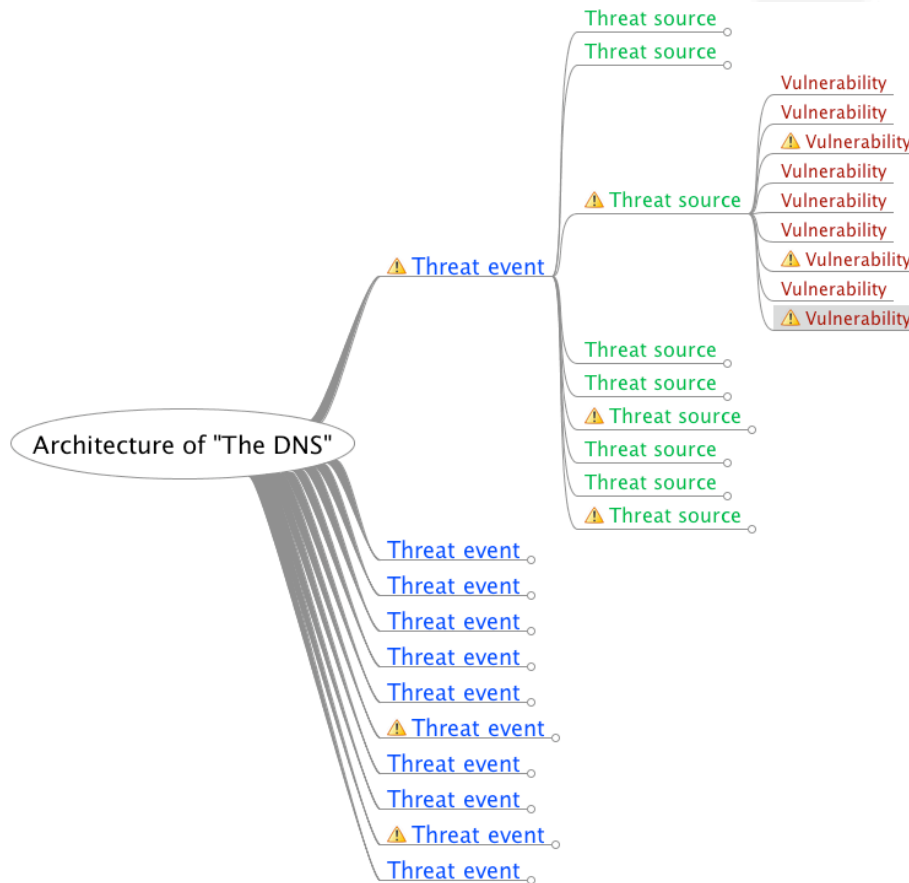
The methodology presumes a tiered approach to the work



- DSSA is chartered to look at the broadest, most general tier
- However it may be useful to pursue one or two deeper, narrower analyses of specific threats once the “survey” work is complete

Problem: the evaluation per NIST methodology does not scale

It's all about choices



- Threat tree could easily grow to over 1000 permutations
- Prune the tree along the way, in order to focus on the highest risks
- Leave a framework that can be used to address:
 - New things
 - Changes
 - Greater detail

Confidential information

Note: Sensitivity, attribution and release to public are determined by info-provider	Sensitive		Not sensitive
<p>Not attributed to source (transmitted through trusted 3rd party or summaries of Type 1 developed by sub-group)</p>	<p>Type 2: Distributed to sub-groups only. (Info-providers determine ultimate distribution)</p>	<p>Info-provider authorizes release</p>	<p>Type 3: Distributed to DSSA and public ("sanitized" info from sub-groups and other non-attributed information)</p>
<p>Attributed to source</p>	<p>Type 1: Distributed to sub-groups only (under NDA, most-protected)</p>	<p>Confidential info must never pass through this path. This is the exposure of information we're trying to prevent.</p>	<p>Type 4: Distributed to DSSA and public</p>