Building a More Trusted and Secure Internet

RIPE 70, May 12 2015

What Must We Trust? (1)

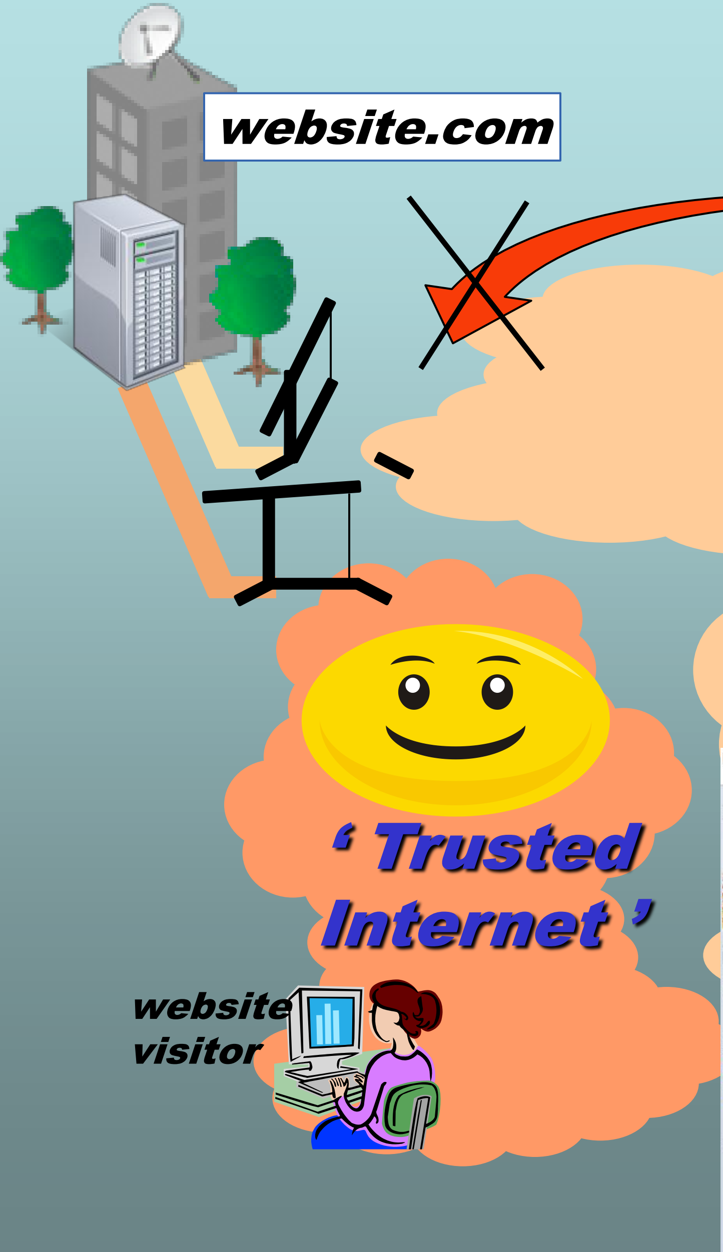
- Steve Bellovin: “For more than 50 years, all computer security has been based on the separation between the trusted portion and the untrusted portion of the system.”
- Once it was “kernel” versus “user” mode, on a single computer
- As systems became more and more distributed, and their number grew enormously, the whole notion of a so-called TCB (Trusted Computing Base) became irrelevant
- http://www.circleid.com/posts/20150217_what_must_we_trust/

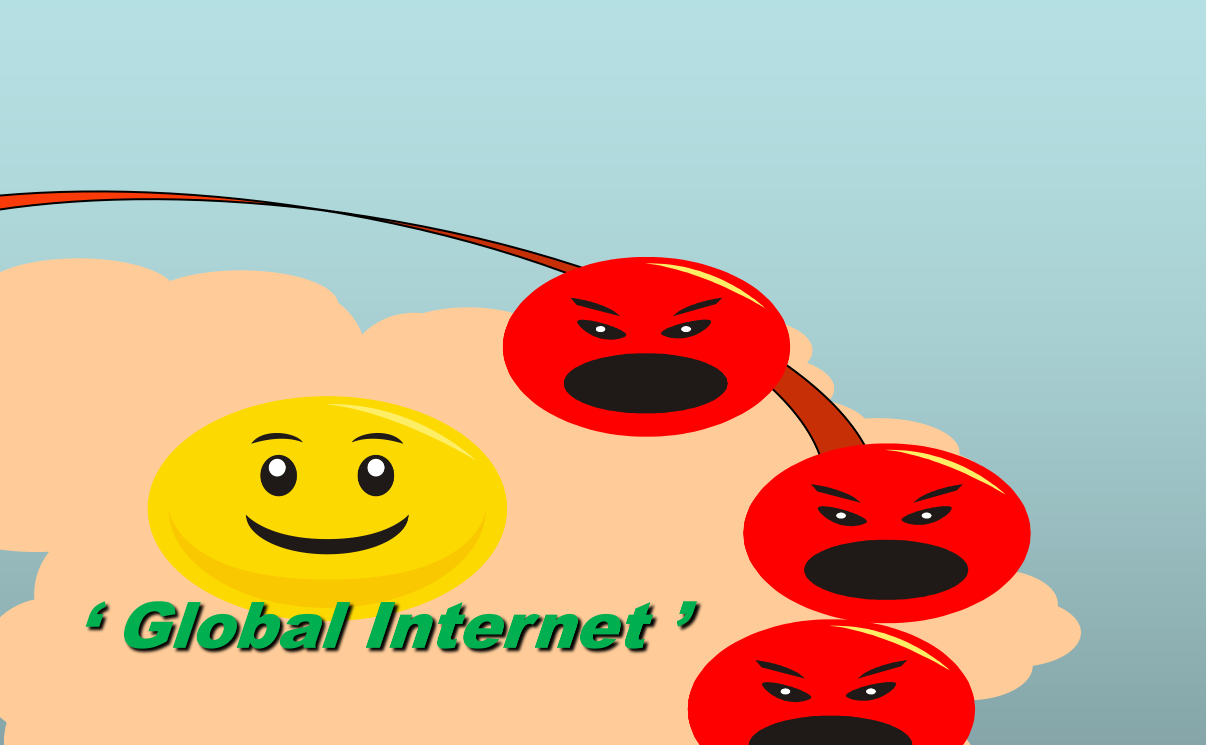
What Must We Trust? (2)

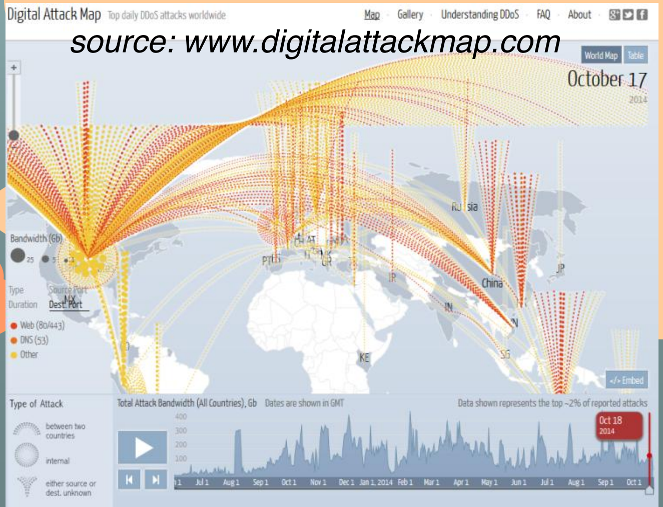
- For networking, once a tight operational community with close collaboration links, the Internet grew into a global communication and information sharing system
  - along with that “trust” deteriorated
  - unfortunately, a lot of network operation is still based on trust
- There is a need to re-enforce trust and the culture of collective responsibility. Can we and to what extent create a Trusted Networking Base today?

‘Trusted Networks Initiative’

A last ‘drawbridge’ in case of (too) big DDoS attacks






Digital Attack Map Top daily DDoS attacks worldwide

Map · Gallery · Understanding DDoS · FAQ · About

source: www.digitalattackmap.com

World Map Table

October 17 2014

Bandwidth (Gb)

Type Source Port

Duration Dest. Port

● Web (80/443)

● DNS (53)

● Other

Type of Attack

between two countries

internal

either source or dest. unknown

Total Attack Bandwidth (All Countries), Gb Dates are shown in GMT

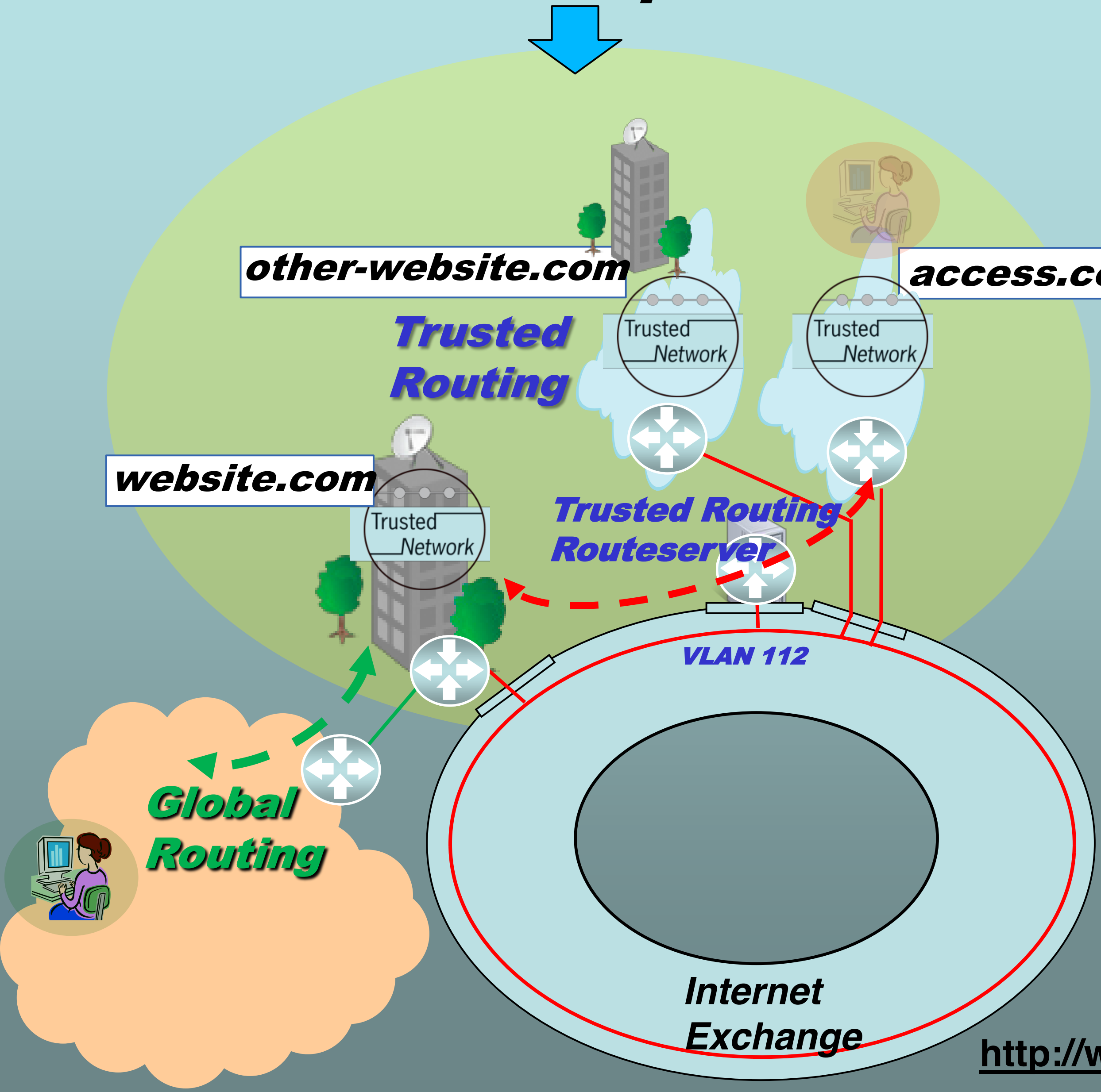
Data shown represents the top ~2% of reported attacks

Oct 18 2014

</> Embed

‘Trusted Routing’

Concept & Policy



a) Take technical measures

b) Take organisational measures

c) Respect the law

Trusted Networks Initiative

http://www.trustednetworksinitiative.nl

FENIX Project

- Separate VLAN at IXP for **secured** networks, last resort in case of huge DDoS attacks, cooperation
- Technical & organizational requirements (BCP-38, full redundancy, CERT team, RTBH, DDoS protection, IPv6, DNSSEC, …)
- Reputation – active participation for more than 6 months at IXP, recommendation, voting

FENIX Project

- Available at NIX.CZ (Prague), NIX.SK (Bratislava)
- Currently 9 members
- Others to come
- Self governance – independent on IXP
- Member meetings
- Security incident sharing and other cooperation
- http://fe.nix.cz/en/

Goal and Vision for GovIX in AT

- Provide a trustworthy platform for entities of public administration and organizations offering important services to them
- Support business continuity in case of general Internet outages and/or during (DDoS) attacks
- Add value to the usual “simple” exchange point components by:
  - Admission control managed by a government entity (and advisory group)
  - Offering (authoritative) DNS Services for the full tree from the **root** through **at.**, **gv.at.** and to individual identities!
  - GovCERT is involved as well
  - Operated by the neutral ACOnet and VIX Team (not a member itself!)

http://reference.e-government.gv.at/Veroeffentlichte-Informationen.2243.0.html

Status of GovIX in AT

Implementation:

- A dedicated VLAN on top of ACOnet's country-wide fiber infrastructure
- Authoritative DNS servers directly accessible from this VLAN
- Configured to be used as the regular, preferred path amongst participants

Experience so far:

- Has proven its usefulness already!
  - e.g. by providing access to the National Citizens Register in case of ISP problems and upstream line outages

Ongoing challenges:

- Logistics within the participating organizations, like
  - Identifying the important services offered to, or consumed from, other entities (to support availability tests and outage management "fire drills"), Identifying and managing the DNS identities used
  - Integrating (an) Austrian Certificate Service Provider(s) – in progress

The Mutually Agreed Norms for Routing Security (MANRS)

- Aka Routing Resilience Manfesto:
  - https://www.routingmanifesto.org/manrs/
- Defines a minimum package: 4 Actions
  - Too many problems to solve, too many cases
- Collective focus and commitment
  - Your safety is in someone other's hands

Good MANRS

1. Prevent propagation of incorrect routing information
2. Prevent traffic with spoofed source IP address
3. Facilitate global operational communication and coordination between the network operators

Panellists

- Jaya Baloo, KPN (chief information security office)
- Ondřej Filip, CZ.NIC [FENIX]
- Marc Gauw, NLnet [TNI]
- Andrei Robachevsky, ISOC [MANRS]
- Wilfried Woeber, Viena University (emeritus DB WG co-chair) [GovIX]

Question 1

a) The focus on the problem the initiatives try to solve

b) And “how”, the approach to the problem

Question 2

Since the ultimate objective is to build a more trusted and secure Internet

a) How are these approaches going to scale up?

b) What are the issues, e.g. technical, logistics, business continuity, …