Internet Engineering under Stress

Secret Working Group report

AfNOG X

May 2009

African Secret Working Group

The Internet

A place where many live, work and play.

A network always under pressures

- **More users, devices and traffic**
- **www, ftp, e-mail, irc, chat, VoIP, Video**
- **Everything over IP !!!!!**

A dangerous place where we can do things safely

- **Innovations at the edge and end-to-end security**

New challenges

The Internet has passed successfully some challenges

- Host.txt ➡ DNS

- Classfull ➡ CIDR

- 13 roots ➡ Anycast

etc...

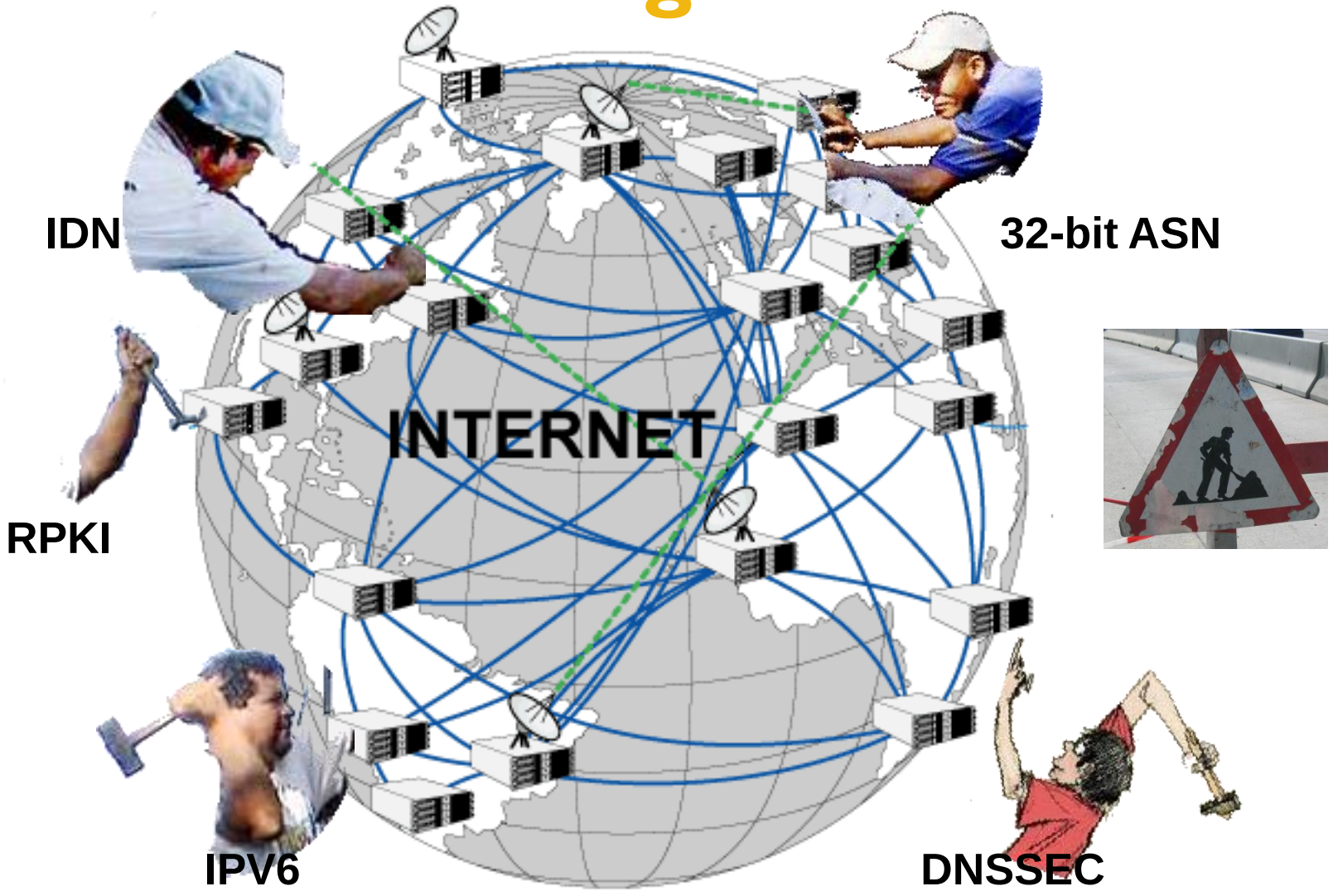
Some new challenges came up

- Securing Internet core protocols

- localisation of the domain names

- Depletion of core resources (IP addresses, ASN)

New challenges



African Secret Working Group

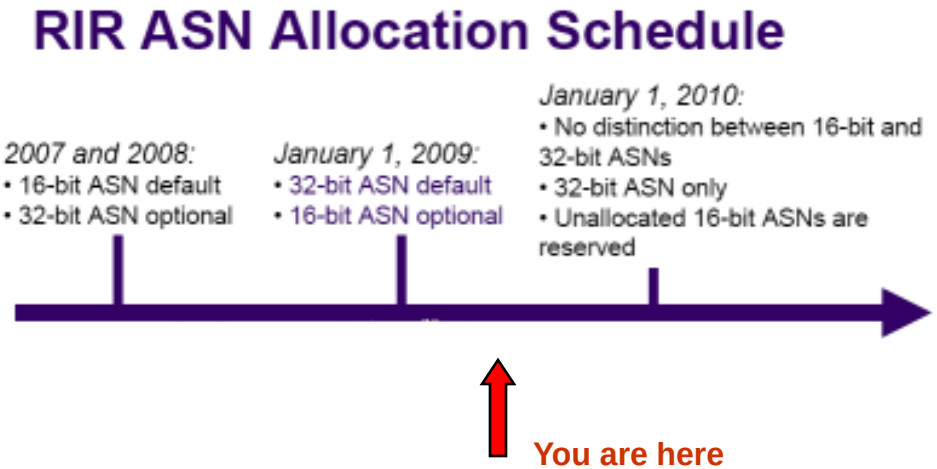
32-bit ASN

16-bit ASN – RFC 1930

Exhaustion: between 2010 and 2011

32-bit ASN – RFC 4893

http://www.afrinic.net/docs/policies/afpol-asn0604.htm



Manufacturers did not follow

African Secret Working Group

IPv6

Billions of hosts allowed in IP4

-Not enough for each person

-Not enough for endpoints

Solution = IPV6

-Transition mechanisms : Dual Stack
-V4 only to V6 only:
NAT- PT DEPRECATED

Aieee we are in trouble !!!

So let's expand IPV4 lifetime
(NAT IS NO LONGER EVIL)
CGN ? DS Lite ? A+P ? IPv4.5?
Explore new NAT-PT
NAT 64 ? DNS 64 ?

- Global IPV6 deployment slower than originally expected

- IPV4 exhaustion getting closer 2011 – 2012

- IPV4/IPv6 transition critical and complicated

African Secret Working Group

IDN

Use of characters other than A(a) - Z(z), 0 - 9 and "-"

Script	Language	SLD.TLD U-labels	SLD A-label	TLD A-label
Arabic	Arabic	مثال.إختبار	xn--mgbh0fb	xn--kgbechtv
Arabic	Persian	مثال.آزمایشی	xn--mgbh0fb	xn--hgbk6aj7f53bba
Chinese, simplified	Chinese	例子.测试	xn--fsqu00a	xn--0zwm56d
Chinese, traditional	Chinese	例子.測試	xn--fsqu00a	xn--g6w251d
Cyrillic	Russian	пример.испытание	xn--e1afmkfd	xn--80akhbyknj4f
Devanagari	Hindi	उदाहरण.परीक्षा	xn--p1b6ci4b4b3a	xn--11b5bs3a9aj6g
Greek	Greek	παράδειγμα.δοκιμή	xn--hxajbheg2az3al	xn--jxalpdlp
Hangul	Korean	실례.테스트	xn--9n2bp8q	xn--9t4b11yi5a
Hebrew	Yiddish	בײַשפּיל.טעסט	xn--fdbk5d8ap9b8a8d	xn--deba0ad
Kanji Hirigana, and Katakana	Japanese	例え.テスト	xn--r8jz45g	xn--zckzah
Tamil	Tamil	உதாரணம்.பரிட்சை	xn--zkc6cc5bi7f6e	xn--hlcj6aya9esc7a

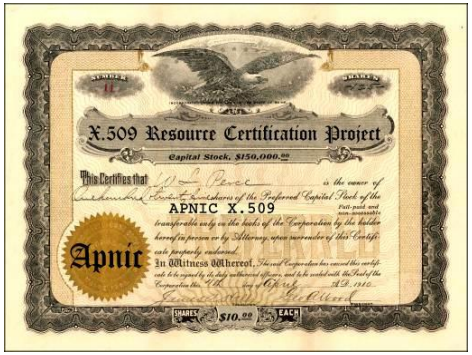
http://xn--mgbh0fb.xn--hgbk6aj7f53bba/" = "http://مثال.آزمایشی "
IDNA2003 Tied to Unicode 3.2

Unicode moved to 5.X : additional scripts available
Experiences show that significant improvement can be made in the protocol
Challenges with the languages written from right to left (Bidi)

OUCH !!!
IDNA2003 need to be reviewed (RFC 4690)
IDNA2008 or IDNAv2?

African Secret Working Group

RPKI



Routing is build on sloppy mutual trust

All trust and no defence

Routing security is pretty bad

Random Whois data

We need routing security

Starting point for routing security:

- Injection of reliable trustable data : RPKI

- Explicit verifiable mechanisms of integrity of data distribution

Can we make decent security and support "better, cheaper and faster " network services?

Isn't it another critical point of vulnerability?

Which trust anchor for the RPKI?

African Secret Working Group

DNSSEC

DNS is a critical part of the infrastructure

DNS was never secured but must be

Secure DNS will provide barrier for DNS based attacks

Secure DNS will provide a security ring around many systems and applications

Solution = DNSSEC

DNSSEC and DNSSEC-bis never get deployed

Kaminsky attacks reminded us how weak is the DNS

OOOuf we need to deploy DNSSEC !!!

Who will sign the root zone?
Who will hold root key ?
How can we distribute and roll root key?

African Secret Working Group

TOO MUCH STRESS

Concentrate Expresso can kill you

Relax a bit and let's think about how we have made it from ARPANET to the current Internet and may be learn from it.

SEE YOU AT AFNOG XI
HOPE YOU WILL MAKE IT

http://african.secret-wg.org

African Secret Working Group