DNSSEC DEPLOYMENT CHALLENGES

Abdalmonem Galila / ICANN-60 / 01-Nov-2017

.masr IDN ccTLD (مصر)
CHALLENGES BEFORE DEPLOYMENT

- What is DNSSEC !!
- How DNSSEC works !!
- From Where should we start deploying DNSSEC !!
- Keys attributes that should be used for signing !!
- Do we have to do changes to registry system before DNSSEC deployment !!
- DNSSEC Secures the communication between master & slaves DNS’s or not
- Firewall should be well prepared before taking DNSSEC into production.
CHALLENGES AFTER DEPLOYMENT

- What is next after deployment
- How to keep our domains active all the time
- Domain re-signing automation
- How often do we have to roll keys
- How to spread the word of DNSSEC to Our Registrars
CHALLENGES AFTER DEPLOYMENT

- One of .masr DNS servers does not respond to TCP queries.
- Response size exceeded 1500 if using both KSK and ZSK for signing.
- DNSSEC also introduces new operational tasks such as rolling the keys and resigning the zone. Such tasks must be performed at regular intervals.
- ISP DNSSEC validation off.
CHALLENGES AS A REGISTRAR

We have 4 registrars, 3 of them are an ISP

- Our customers do not have idea’s about DNSSEC
- Hard.
- System is stable so why we have to change
  - More time required to resolve domain name
CHALLENGES AS A REGISTRAR

- Domains with invalid signatures will be blocked.
- Attacks on the DNS are too rare to raise concerns
- We have many attacks and we can mitigate it
- Registrants do not have an idea about DNSSEC
- No enough staff to monitor & troubleshoot DNSSEC
DNSSEC Zone *Signing Automation
Script For .masr (مصر)
SCRIPT STRUCTURE

1. Script Initialization Inputs
2. Unzip Registry Generated Zones
3. Apply Checks
4. Loop Zones
5. Sign Zones
6. RNDC Reload
SCRIPT ELEMENTS SAMPLES

my $srccdir = ' ';  
my $srccdir = ' ';  
my $srccdir2 = ' ';  
my $tmpdir = tempfile(CLEANUP => 1);  
my $signDir = ' ';  
my $filesizedelta = 0.50;  
my $salt;

my $change = abs(($stat_cur_file->size - $stat_prev_file->size) / $stat_cur_file->size);  
if ($change > $filesizedelta) {  
bail("File size changed by greater than $filesizedelta percent! Bailing out!");
}

print "Using file: $cur_file\n";

# Now we unzip them  
chdir $tmpdir;  
system("unzip -q $cur_file");

foreach my $zone (@zones) {  
    my $name = split('\\.', $zone);  
    my $tld = pop $name;

    eval {  
        system("sed -e 's/^\//g' $tmpdir/$zone.zone > $dstdir/db.$zone");  
        system("sed -e 's/^\//g' $tmpdir/$zone.zone > $dstdir2/$zone.zone");  
        system("chgrp named $dstdir/db.$zone");}
55  system("cat $signDir/Keys/Kxn--wgbh1c.c+008+*.key >> $signDir/UnSigned/Kxn--wgbh1c.zone");
56  system("/usr/sbin/dnssec-signzone -d $signDir/Signed/ -3 @salt -e +30day -x -x $signDir/Keys/Kxn--wgbh1c.zone");
57  print "DotMasr is already signed Now";

69  sleep(5);
70  system('/usr/sbin/rndc reload');
71  print "Run complete at ";