Council of European National Top Level Domain Registries

Report on IETF 87 Berlin

29 Jul - 5 Aug 2013

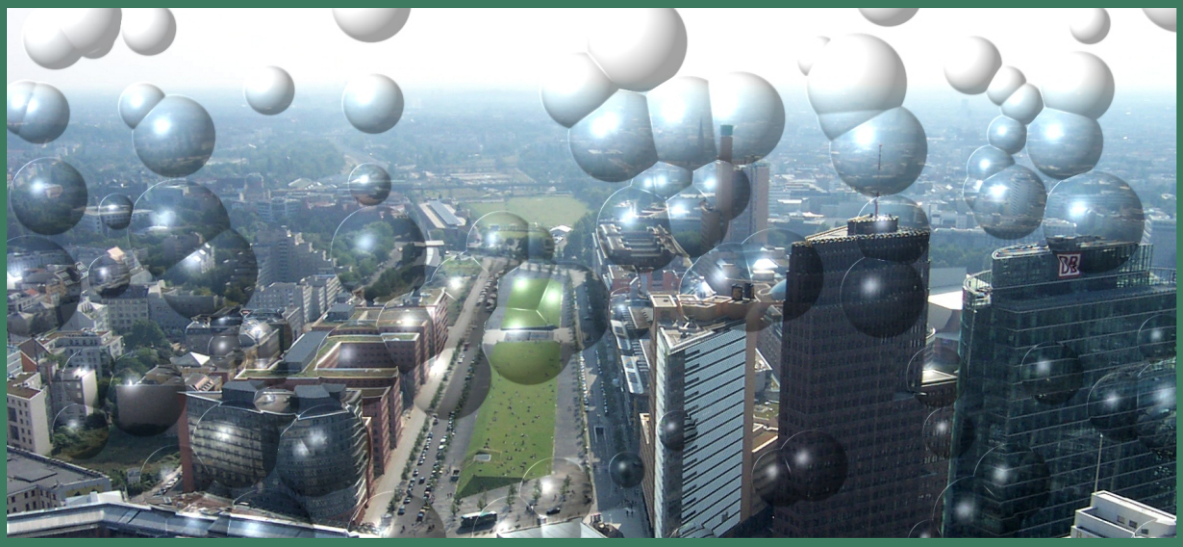

Table of Contents

Highlights

No escape for IETF from mass surveillance revelations: Tor@IETF

The Tor Project was presented at the IETF 87 by computer activist Jacob Appelbaum amidst a new round of revelations from Edward Snowden, the former Booz Allen Hamilton employee who stripped naked several large-scale mass surveillance programs of the National Security Agency, NSA, and the British GCQH. In an adhoc session Wednesday night Appelbaum analyzed the file deck on Xkeyscore (a several day TCP-dump of Internet data collected on more than 500 servers located all over the globe and allowing searches over the collections).

He announced during the Wednesday night session and also in a talk on Tor during the Security Area that he would document the Tor server network in an informational IETF Request for Comment (RFC) and asked for support from the IETF community to increase and harden the network.

Ideas discussed as an answer to the mass surveillance include the mandating of strong (according to Appelbaum ephemeral key) encryption in all IETF protocols. In general a revisit of the susceptibility of IETF protocols to surveillance should be started, Appelbaum recommended. Encryption helps, Appelbaum said. This was made clear in the documents revealed by Snowden, because encrypted traffic was addressed as a special target.

IETF Danvers doctrine, laziness (at least) in implementing strong encryption and ties to intelligence community

Closer monitoring and analysis of security problems in protocols and operations are should be established by the technical community. The IETF has work underway on certificate transparency (RFC6962) that allows to monitor broken certificates for everybody. Appelbaum proposed a working group (or something similar) that would share analyze traffic data considered to come from state hackers. IETF participants asked for documentation of the various state attacks on Tor for example. Disguised attacks on the net have also been observed by operators present at the IETF, including the ccTLD community.

The Chair of the Internet Architecture Board, Russ Housley when asked for a reaction to the mass surveillance programs during a press conference at the Berlin IETF pointed to the IETF's Danvers Doctrine (documented in RFC 3365). Housley, owner of the small security consultancy Vigil Security, has been sponsored for both his chairmanship of the IETF and, now, IAB by the NSA illustrating the strong ties by technical community and US agencies.

The Danvers Doctrine is a consensus by the IETF community to use strong use strong, instead of weak („export“) encryption in IETF standards. Yet the IETF often did not include the stronger protection in the standards, but made it only one option. A recent example is strict transport layer security which will not be a „MUST“ in http-bis. One counter-example from Berlin on the other hand is the decision against using keys stored at platform providers for WebRTC browser to browser calls (see below Web RTC WG).

During an extensive discussion at the Tor presentation and the Security Area Open Meeting it was agreed that potential joint work would be developed on a new, dedicated mailing list.

On traffic monitoring work was presented in Berlin at a workshop of the Network Monitoring Research Group. A presentation by the University of the German Forces for example described „an approach for correlating flow data“. Endpoint assessment and continuous monitoring of systems are furthermore discussed in a new WG, the SACM WG, which has been pushed for by several US bodies, including the National Institute of Standards Technology (NIST) and the DHS (see below SACM WG).

WGs and BoFs

STIR BoF - Secure telephone identity revisited, a US problem only?

Given the overwhelming support for securing identity across the different networks (IP, SS7) it can be taken for granted that STIR will become a new IETF WG. It will address abuse of security gaps in IP networks allowing for spoofing existing or non-allocated Ids (numbers) for attacks like robo-calling (automatic telemarketing), denial of service (on parties not willing to pay ransom) or phishing calls (smal number of 'swatting' cases).

Earlier attempts to secure identity have failed, public ENUM (which could have allowed for attached certificates) failed. During the BoF Henning Schulzrinne, FCC CTO, presented the problem statement (see also lenghty draft from Jon Peterson, of US phone registry provider Neustar), asking for a quick solution while acknowledging an incremental deployment.

Starting in the 01-region (North America) only and neglecting international robocalls made sense, he said. Waiting for international implementation would mean to lose time. Threat models anyway differ depending on regulation and market situation – robo-calling in the US is used heavily, and also in some instances legitimate, as one participant underlined.

Cases to be dealt with include SIP to PSTN, PSTN to SIP, IP to PSTN to IP, and more. The future WG will have to decide if validation should happen in-band or out-of-band. Discussions in Berlin were inconclusive as to which of the two could be faster deployed. Given that there were existing solutions for example for i-message (Apple) out of band would be deployed faster, said Cullen Jennings (Cisco). In-band would beat out of band, said Martin Dolly from AT&T Labs. Klaus Nieminen from the Finnish Regulator Ficora said, mobile providers could validate VoIP in band. In-band was preferred.

Out-of-band validation can create considerable privacy problems, with an additional third party being able to see which numbers were called from a phone.

SACM WG - Security assessment and continuous monitoring

The WG has been created despite some concerns stated after their second BoF meeting at the IETF Orlando. The declared goal of the WG is to get interoperability between tools helping to allow for automatized security posture assessment of enterprises/organizations. While there seemed to be an agreement to narrow the focus on the security posture assessment of end-points in an enterprise system, the use list presented by Dave Waltermire (NIST) is still kept open as use case 2 and 3, „enforcement of acceptable state“ and „security control verification monitoring“ respectively.

Additional detailed use case has now been fleshed out in the draft by Dave Waltermire (NIST) e.a. Including „suspicious endpoint behavior, vulnerable endpoint behavior, batch assessment, event driven monitoring and periodic monitoring.“ There were already many vendors offering monitoring solutions resembling to what the WG seemed to have in mind, one WG member noted. Vendors were therefore well respected during the session in Berlin. Despite potential clashes with existing solutions the WG should not go out to other events to „market“ the draft solution.

PKI over TLS (***POSH***)

As long as Dnssec and Dane is not deployed there is a problem to start secure SIP or Jabber (XMPP) connections where they are on hosting platforms. A BoF initiated by Peter St. Andre and Matt Miller (both Cisco) presented what some called a „hack“ to address the gap.

The core problem presented by St. Andre and Miller is that certificates do not extend from a source domain over subdomains, therefore authentication of a an end point is difficult when starting a Transport Layer Security-protected

(TLS) session. The option to have keys stored at the hosting provider to allow for authentication of the user in the delegated domain

There is a possibility of store keys at the hosting service. But neither might customers be willing to share their private keys with the hoster, nor might hosters be prepared to take on the responsibility to manage and store their customer's keys.

The POSH concept will according to the document authors allow to close the gap by presenting a requesting server with a Jason Web Key (JWK), a „Javascript Object Notation (JSON) data structure that represents a public key". JWK is currently under discussion in the JOSE WG. When the authentication via the https server of the source domain was successful the secure connection can be started.

One downside of the idea is that for securing http there is a bootstrapping problem. Nevertheless there was considerable support for the idea during the BoF.

SIDR

More tools for the management and validation of Routing PKI, and also for its monitoring will help to push deployment of secure routing. One of the pre-events to IETF Berlin, organized by the Free University of Berlin (Matthias Waehlisch and others) was dedicated to RPKI deployment and gaps. Interest was considerable according to the organizers. Deployment while showing faster adoption rates that Ipv6 (for example) is still slow, with the ARIN region being the trailer (0,14 percent RPKI adoption rate, see below). Large operators including Deutsche Telekom, Facebook or Mozilla have started to protect their Praefixes, said Matthias Waehlisch, FU Berlin.

RIR	Total	Valid	Invalid	Unknown	Accuracy	RPKI Adoption Rate
AFRINIC	11256 (100%)	16 (0.14%)	39 (0.35%)	11201 (99.51%)	29.09%	0.49%
APNIC	117349 (100%)	85 (0.07%)	214 (0.18%)	117050 (99.75%)	28.43%	0.25%
ARIN	183166 (100%)	224 (0.12%)	31 (0.02%)	182911 (99.86%)	87.84%	0.14%
LACNIC	56913 (100%)	5517 (9.69%)	1148 (2.02%)	50248 (88.29%)	82.78%	11.71%
RIPE NCC	129120 (100%)	6503 (5.04%)	1151 (0.89%)	121466 (94.07%)	84.96%	5.93%

These figures have been generated by a global RPKI monitoring project from Surfnet (see here).

Operators and RIRs were able to use the dashboard to check on the adoption of RPKI, invalids and configuration mistakes, detailed prefix information on a daily base. More tools were presented from the LACNIC labs, for example, an RPKI Origin validation looking glass (to use for monitoring, manual checking or , a ROA Wizard (allowing for the generation of ROAs) including a ROA to BGP prefix converter. More tools are also available from the FU Berlin/H Hamburg group which is focusing on prefix origin validation with a „RTRlib" (allowing to be used on Quagga routers or just for monitoring), available since 2011.

There was still a gap in available tools to make RPKI useful for those not able or willing to run origin validation in their own routers, the experts agree. Alternative use cases for the information already stored in the RPKI should be encouraged according to Carlos Martinez Cagnazzo (LACNIC) and Benno Overeinder (NInet Labs). Some centralized library (as for example was available for DNSSEC here) could be nice to get a better overview on RPKI tools.

One tool discussed more intensively during the first of three SIDR sessions was the proposal of a new version of the

Localized Trust Anchor Management (LTAM 2) proposed by Steve Kent (BBN). LTAM shall allow to handle BGP validation – and having ones „individual view“ of the routing tables. Now two additional aspects need to be addressed with LTAM2 according to Kent. LTAM 2 shall allow an operatort to assert ownership of a prefix (for example for private addresses). It shall also ease concerns from governments that certificates for critical infrastructure might be invalidated maliciously. A nation could protect itself in its own jurisdiction against such moves by directing internal nets to „rely on a national authority for RPKI data for these critical infrastructure resources“.

From the Kent's idea that countries should be able to declare the respective ROAs externally also it is only a small step to a nationalized routing table view, something that opponents of RPKI see as a potential censorship tool. Interestingly, so far the possible „political attack“ was expected to be „law enforcement or rights holders against alleged criminals“. Given Kent's proposal RPKI looks like armor for cyber warfare, but Kent so far has no written draft. There could be a need for a design group, Randy Bush, Internet Initiative Japan said after the meeting.

During the Berlin meeting several experts told this reporter, it was the Chinese ministry that was concerned as the registry for its resource certificates was in Australia (APNIC). Needless to say that a centralized (US-based) trust anchor seems nothing that would be easily accepted globally. Policy (layer 9 problems) certainly were a barrier to RPKI deployment, Waehlisch said.

WebRTC: strong, not weak encryption of browser to browser calls

The WebRTC working group after delaying it several times in Berlin decided to make strong security a must in browser to browser calls. The Datagramm Transport Layer Security Secure Real Time Protocol (DTLS-SRTP) had been selected as a must implement-feature for the WebRTC protocol suite, but companies like Skype/Microsoft had requested optional status for the alternative Security Descriptions protocol (SDES) as well.

SDES especially is helpful for „out-calls“ from IP to non-IP connections. The WG after a heated discussion decided that SDES „MUST NOT“ be used for WebRTC.

The main reason for the decision is a perceived vulnerability of SDES to surveillance. Eric Rescorla, author of DTLS in a comparison of both protocols explained that authentication keys in SDES would be managed by the siginalling server, to ease key handling. DTLS demands a negotiation of keys at the end points, using the Diffie-Hellman-concept (Chrome and Firefox already implement this). The latter demands an active attack on the connection in order to tap the conversation. SDES according to Rescorla on the other hand enables passive snooping, as keys are available at the signaling server, communication therefore even can be reconstructed retroactively.

Given this security weakness even one of the SDES authors, Dan Wing, was decidedly against allowing SDES as an alternative option, as people could use the weaker, less onerous protocol as default (see Wing's earlier analysis of the weaknesses here). WebRTC co-chair Cullen Jennings said to this reporter, the WG had even before the recent surveillance revelations tended to decide against SDES.

The WebRTC which is preparing the framework to allow seamless real-time communication via browsers according to a status report by co-Chair Jennings has pushed many of the specifications for the framework up to 70 or 80 percent. The audio codec Opus developed specifically for WebRTC was presented during the technical plenary as a success story for IETF standardization. The WG achieved to combine competing proposals like Silk and Celt to make Opus a broad specification for both language and music. Not only did Opus support flexible bitrates (6 to 510 Kbit), flexible sampling frequencies (8 to 48 kHz) and flexible audio-frames (2,5 to 60 milliseconds). The WG also pushed for a BSD license – in a field that is a minefield of patents. The battle about the video codec for WebRTC is still underway with Google pushing for VP8 successor VP9 and Nokia filing an IPR disclosure statement challenging the VP8 RFC (RFC 6386). The WG did not discuss the video issue in Berlin, but heard additional presentations on security.

DNSOP - operators would love a „panic button“

The DNS Operations WG is getting more work, with all of the proposals presented during the Berlin meeting tentatively accepted as interesting work items. The most debated new knob for the DNS: a big red panic button to flush caches in case of „emergency“ - for example problems with DNSSEC key rollovers. Joe Abley, ICANN, proposed the panic button – which in fact is supposed to facilitate an authenticated, non-manual mechanism to request cache flushes for particular domains with „significant cache operators“. Abley said „Notify“ could be used to trigger the flushes, even if this was a „hack“ (NOTIFY to auth server: invitation to AI XFR, NOTIFY to recursive server flush cache for indicated domain). The problem to be solved was the load of cache renewals operators did manually on hearsay (mailing list announcements) that a domain was in trouble. While a „panic button“ itself was welcomed by many, the hack option presented did not get a lot of support and many warnings with regard to scalability, potential censorship, complexity problems.

Work welcomed during the session included how to keep AS112 servers up to date with regard to added or dropped zones. Beside the already discussed omniscenet AS112 concept (see draft here) Joe Abley proposed to use DNAME (zone aliasing) redirection. Instead of delegating individual zones to AS112 DNAME shall allow querying for the junk domains without reconfiguration of the AS112 servers. Both documents will be developed in parallel for the time being.

Another duo of approaches will go forward on how to handle DNSSEC key handovers from children to parents. As children do not „speak“ EPP other options how to securely organize the handover have to be explored. The two presented at th Berlin were CDS (Kumari, Google, e.a.) and CSYNC (Hardaker, Parsons, e.a.).

The CDS resource record which holds an updated DS key for the child zone can be used by the parent zone to update an existing key. „If at least one DS and one CDS record exist (at the child zone apex, signed with current key), the parental agent validates and then copies the contents of the CDS RRset and replaces the entire existing DS set with the new one.“ (see draft). The alternative Child to parent synchronization in DNS (CSYNC) would also introduce a new resource record, that would more generically indicate „which delegation records within a child should be processed into the parent's DNS zone data.“

The more generic nature (not only DNS keys, but also name server and glue records. The difference between the two is mainly that CDS puts the DS key into the child while CSYNC points parent as to what to copy. While there were proposals in the discussion to use CSYN for unsigned records, but CDS for DS records (Matthijs Mekking, NInet Labs), others found CSYN was preferable as more generic (Ondrej Sury, Cz.nic). There were also critical comments that CDS implied a preference for a specific policy (Antoine Verschueren, SIDN). While the existing split of DS records and DNS keys would persist, DNSOP should not pave the way for further split, participants warned. Both proposals received close to unequivocal support in a hum and will proceed in the WG.

The DNSOP WG has a new co-chair: AOL Sr. Network Engineer Tim Wicinski. There had been considerable interest for the position as over a dozen people had volunteered for it according to Area Director Joel Jaeggli. Tim Wicinski has not been very active as a document author.

DANE

The DANE WG discussed two current practice/implementation guideline documents from Victor Dukhovni. One looks into DANE use for SMTP, another into more general „lessons learned“, including a potential clash of the DANE and the new experimental transparency spec.

General problems existing are large key sizes (use hashes!) that also provide for amplification attacks, the existence of CNAME (use server name indications!). Dane type specific guidelines were discussed. Type three (self-certificate in DNS, no CA) is least likely to fail. Type 2 (fingerprint at CA) needs publication root trust anchor in certificate chain, right now practice was that there was no need to publish.

A major discussed covered the potential clash of Dane and the certificate transparency document (which wants to hold certification authorities accountable). „If the CA is not a public CA, or DANE TLSA RRs constrain the end-entity certificate to a fixed public key, there is no role for CT, and clients SHOULD NOT apply CT checks“, is the major recommendation. A mixing of Dane models was dis-encouraged, said Wes Hardacker presenting the drafts. Discussion between certificate

transparency and Dane people is necessary, IAB Chair Russ Housley said.

With regard to SMTP (which could be merged with an existing draft) Dukhovni concluded from implementation in postfix that DNSSEC plus DANE allowed to „harden MX lookup via DNSSEC, provide downgrade resistant TLS support, publish authentication public keys digest or keys". Yet SMPT TLS security was dependent on DNSSEC, if DNSSEC is broken „all bets are off". Some MTAs according to Hardacker have announced to map DANE models (0-2 and 1-3).

Should the IETF implement DANE for its own email? Peter Koch from DENIC eG cautioned, but experimental usage first to expand over all IETF email was welcomed.

Precis

The Precis WG after being close to finalization of its main documents discussed to go on setting up a directorate in order to answer future questions on normalization and case mapping brought up. The stream of such questions was not expected to dry, but no full WG was needed.

IETF Administrative

Record number of first-timers, Chairs' review and diversity

The Berlin meeting was one of the largest meeting in recent time (1426), and according to new IETF Chair Jari Arkko attracted more countries than any other meeting of the IETF (62). Berlin while having only one platinum sponsor (DENIC eG) and several gold sponsors (EURid, DTAG) also set a record with regard to first-time attendees to an IETF meeting (316).

Arkko in a short review of the meeting on the IETF Chair blog – which he started – welcomed „newcomers from the root server operator community, network operators from developing countries, regulators and policy makers, ICANN specialists and students." ISOC sponsors several programs to bring new attendees to the IETF. Interesting to note that a representative of the German government (not exactly a poor developing country) was also invited to participate in the government program.

Two German Universities (Free University of Berlin and University of Applied Science in Hamburg) had brought large groups of their students to the meeting after having obliged each of them to write reviews for drafts to be discussed in the Berlin meeting on topics they do research on. „The influx of new people is important", Arkko blogged, „to make sure that we understand the challenges in all aspects of Internet technology." Work on diversity is also ongoing and was discussed during the administrative plenary meeting.

Postel Award

Elisabeth „Jake" Feinler was awarded the Jon Postel Award 2013. She had been Director of the Network Information Systems Center at Stanford Research International for the Arpanet, in charge of the Network Information Center (NIC) for the just developing Internet. Feinler had been working directly with Postel („a nice guy moved in"), until he left for the Information Services Institute (ISI). The NIC stayed at SRI and helped baptize the new gTLD zones and manage several of them including mil, gov, edu, org and com after the DNS was introduced to scale addressing. During the Orlando meeting Feinler proposed an IETF history group to collect documents and even pieces of hardware for the Computer Museum. Her motto, she reiterated in Berlin, was „do not throw it away, it's history". Feinler is the 14th Postel awardee (see the list).

Is an RFC a Standard?

During both the technical and the administrative plenary the concern about a possible clash of IETF nomenclature and procurement policies in some jurisdictions was brought up by Olaf Kolkman, NInet.labs. Kolkman participates in the EU Multi-Stakeholder Platform on ICT Standardization which has been tasked by the EU Commission to screen standards developments in standardization bodies like the IETF.

To make a standard mandatory in public procurement there was a need for stable and accepted standards. The IETF on the other side spoke of its „standards" as „request for comments" and had a two step-process from proposed standard to internet standard. When making Ipv6 a „Must" in EU procurement the fact that it was only a proposed standard was neglected, for less obvious specifications there might be a problem.

One step taken by the IAB now was to post a matrix on the areas the EU wants to see developed and the IETF work in these areas. How the potential misnaming problem will be resolved is open.

Next meeting will take place in Vancouver, 3 - 8 November 2013