Trust by Demonstration ... in a coordinated way

Security Coordination Communications Challenges – all in it together

David Groep
AARC Community, policy and best practice area
Nikhef PDP programme

Nikhef

WISE Community meeting
October 2021
Many communities test, test, and test again
Frequency of challenges and tests - examples

**Trusted Introducer and TF-CSIRT**
- 2-3 Reaction Tests per year
- supported by web click infrastructure, but requires (team) authentication

**SURFcert challenges**
- annual response challenges, just reply to email to a (traceable) ticket

**IGTF RAT Communications Challenges**
- every 1-2 years, in parallel with continuous operational monitoring

**EGI CSIRT Security Service Challenges**
- every ~2 years, aiming at remediation, forensics, and response to real-life (botnet) incidents
Challenge elements – what is valued or expected might differ …

A single test and challenge can answer one or more of these questions

- timeliness
- ability to take action
- confidentiality
- investigative capability

- when data available: infrastructure can set its own level of expectancy and gives deep trust
- assessment supported with community controls (suspension) gives a baseline compliance

Communications challenges build ‘confidence’ and trust – an important social aspect!
- different tests bring complementary results: responsiveness vs. ability act, or do forensics
- unless you run the test yourself, you may not be growing more trust in the entities tested
- for a ‘warm and fuzzy feeling of trust’, share results: but this is sociologically still challenging …
IGFT RATCC4 Results

In total there are 91 trust anchors (root, intermediate, and issuing authorities) currently in the accredited bundle, managed by 60 organisations.

Of the 60 organisations, 49 responded within one working day (82%), representing (incidentally) also 82% of the trust anchors.

Within a few days more, 3 additional ones came in, and 4 more responded after a reminder.

In total, 90% of the organisations responded to the challenge, representing 88% of the trust anchors.

PS: of the non-response organisations, 4 had their public contact meta-data fixed, and 2 were withdrawn from the distribution.
Many RedTeaming tools are now standard (like Mythic C2)

containerisation aids in getting the payloads working across a heterogeneous infrastructure

previous exercises ran into problems with the encrypted binaries and process hiding techniques

integration with the operational submission systems remain

as well as monitoring and report-out
WISE SCCC-WG – participate!

WISE Community:

Security Coordination Working Group:

Introduction and background:

Maintaining trust between different partners and their responses by all parties involved. In a world of distributed, coordinated e-infrastructures, there is a need for well-defined contact information, and have either a trusted contact or an agreed level of confidentiality maintenance. The idea that an unverified becomes stale: security coordination infrastructure may later bounce, or no longer usable. One of the ways to ensure contacting is to have them compare their performance against others.

Campaign information:

Campaigns target different constituencies and may overlap. The description of the constituency given here should be sufficient for a high level of generalisation. If the user wants further information, they should contact the campaign leader for a more detailed description or a list of addresses (which would be a privacy concern since this page is public). Challenges can also probe different aspects of the constituency, as the full cohort may not be available for all challenges, and different perspectives are needed to ensure that the results are effective.

IGTF-RATCC4-2019

<table>
<thead>
<tr>
<th>Campaign</th>
<th>IGTF-RATCC4-2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Period</td>
<td>October 2019</td>
</tr>
<tr>
<td>Initiator contact</td>
<td>Interoperable Global Trust Federation IGTF (<a href="mailto:rat@igtf.net">rat@igtf.net</a>)</td>
</tr>
<tr>
<td>Target community</td>
<td>IGTF Accredited Identity Providers</td>
</tr>
<tr>
<td>Target type</td>
<td>own constituency of accredited authorities</td>
</tr>
<tr>
<td>Target community size</td>
<td>~90 entities, ~60 organisations, ~50 countries/economic areas</td>
</tr>
<tr>
<td>Challenge format and depth</td>
<td>email to registered public contacts expecting human response (by email reply) within policy timeframe</td>
</tr>
<tr>
<td>Current phase</td>
<td>Completed, summary available</td>
</tr>
<tr>
<td>Summary or report</td>
<td>Preliminary result: 82% prompt (1 working day) response, follow-up ongoing</td>
</tr>
</tbody>
</table>

WISE, SIGISM, REFEDS, TI joint working group

see wise-community.org and join!

https://wiki.geant.org/display/WISE/SCCC-JWG

co-chairs: Hannah Short (CERN) and David Groep (Nikhef)
Thank you

Any Questions?

davidg@nikhef.nl

https://aarc-community.org

© members of the AARC Community.

The work leading to these results has received funding from the European Union’s Horizon 2020 research and innovation programme and other sources.

This work is part of a project that has received funding from the European Union’s Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2).

We thank the following sources: EC Horizon 2020 projects GN4-3, EOSChub, and AARC-2; and the Dutch National e-Infrastructure coordinated by SURF.
The SCCC Working Group – a joint effort of many

Coordination of ‘CCs recipient groups’ among participating infrastructures
• ensure targets are not overloaded by coinciding or overlapping challenges, for example by designating lead agency

Transitivity of trust based on challenge frequency and results
• for example by specifying the level of disclosure detail for CCs
• as extension: could CCs be requested e.g. in response to changed risk assessments between infrastructures?

Definition of CC models and classification
• ‘depth’ of the CC testing is a balance between the level of trust gained (more profound testing and good results gives more trust) and expediency (asking mail or click response consumes less resources than requesting forensics of simulated incident)

Frequency of CCs
• simple communications challenges are often performed one or several times per year
• complex challenges are less frequent (e.g. ‘black-box traceability’ trials in EGI take place once every 1-2 years)
• following a CC model classification, propose an appropriate frequency for each class