Trust by Demonstration ... in a coordinated way
Security Coordination Communications Challenges – all in it together

David Groep
WISE SCCC-JWG & AARC Community,
Nikhef Physics Data Processing, UM Dept. of Advanced Computing Sciences

TNC22 Security Day - WISE Community
June 2022
Many communities test, test, and test again
Not all tests are created equal ... and not run equally either!

**Trusted Introducer and TF-CSIRT**
- ~3 Reaction Tests p/year, supported by web infrastructure, (team) authenticated responses

**SURFcert challenges for the national (federated) contacts**
- annual response challenges, just reply to email to a (traceable) ticket

**Communications Challenges: IGTF RAT, eduGAIN-to-federation-ops, EOSC Core providers ...**
- periodic, from every 1-2 years, to annually
- usually 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
- requires much more preparation, and integration with research workflow systems costly
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 (even 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 ...
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PS: of the non-response organisations, 4 had their public contact meta-data fixed, and 2 were withdrawn from the distribution.
Designing challenges for new targets: the European Open Science Cloud

Distance between operational security and (exchange) services remains large

- **who to target first in an open ecosystem?**
- **raising awareness as well as improving response**

Core services easier to identify

- security contact are in place
- service management system is known
- on-boarding process being rolled out

- but designing the security scenarios is an art in itself (thanks to Pinja Koskinen and Alf Moens!)
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

Upcoming EGI SSC challenge ... simplified (with the Mythic C2)
Designing forestics-oriented challenges is exhilarating in itself.

imagery: SSC5 Oscar Koeroo, Graeme Stuart, EGI CSIRT team, WLCG, et al.
WISE SCCC-WG – participate!

WISE Community:
Security Coordination Working Group

Communications Challenge planning
Created by David Groep, last modified by David Groep - STFC UKRI on May 25, 2021

Introduction and background
Maintaining trust between different responses by all parties involved. An integrated and coordinated e-infrastructures, the cross-domain mechanisms, contact information, and have either a defined level of confidentiality and integrity and verified becomes stale: security coordinators of e-infrastructures may later bounces, to ensure contact information is accurate and up to date.

One of the ways to ensure contact information is accurate and up to date is to compare their performance against different campaigns.

Campaigns
Campaigns target different constituencies and may overlap. The description of the constituency given here should be sufficient for a human to assess if there is a detailed description or a list of addresses (which would be a privacy concern since this page is public). Challenges can also probe to different ‘depths’ in an effort not bounce, so testing if the organisation contacted can do system memory forensic analysis and engage effectively with LE. The proposed rough classification is:

- ability to receive – mail does not bounce or phone hangs
- automated answering – ticket system receipt or answering machine
- human responding – a human (helpdesk operative) answers trivially (e.g. name)
- human, fully informed – a human (helpdesk operative) answers and engages effectively

Campaign information

<table>
<thead>
<tr>
<th>Body</th>
<th>Last challenge</th>
<th>Campaign name</th>
<th>Next challenge</th>
<th>Campaign name</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRIS</td>
<td>-</td>
<td>~Q3 2021</td>
<td>IRIS Comm Challenge 2022</td>
<td></td>
</tr>
<tr>
<td>IGTG</td>
<td>October 2019</td>
<td>IGTG-RATCC4-2019</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EGI</td>
<td>March 2019</td>
<td>SSC 19.03 (8)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trusted Introducer</td>
<td>August 2019</td>
<td>Ti Reaction Test</td>
<td>January 2019</td>
<td>Ti Reaction Test</td>
</tr>
</tbody>
</table>

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)
Making the SCCC JWG a useful place for all

• How to grow the community and leverage the trust built?

• Can we use joint machinery for running challenges?
  
  *eduGAIN, EGI, TI, SURF all have tooling, and more is coming*

• The Wiki page is a start – evolution and completeness requires you!
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.