Contribution ID: **53** Type: **Oral Presentation**

Global operational security in collaborating distributed infrastructures

Tuesday, 25 August 2020 15:00 (30 minutes)

Since the Stakkato Incident (https://en.wikipedia.org/wiki/Stakkato) in 2004, it is well understood that incidents can spread quickly over infrastructures with a shared user community. With the advent of federated identity management, the likelihood of incidents "hopping" from one infrastructure to another has increased.

In 2004, the attacker took advantage of the fact that the security teams at the affected infrastructures had only limited opportunities for a coordinated response, and that the infrastructures were rather isolated with regard to policies and procedures. As a result, the incident response happened primarily at the local level.

During the setup of large federated computing infrastructures like EGI and OSG, security was an important component and the readiness of the infrastructures to respond to an multi site incident were assessed in various scenarios. An increased understanding of the implications of a compromised account in a federated identity management system, which gives a miscreant access to multiple distributed IT infrastructures, along with communities and frameworks like WISE and SIRTFI, aimed at harmonizing the security policies across infrastructures, have helped to build an environment where a coordinated incident management is possible.

EGI and OSG already provide operational security to infrastructures that share large user communities. Even so, we may face a similar situation to the infrastructures in 2004, since the anticipated methods of collaboration in an incident affecting EGI and OSG are not yet fully tested.

In this presentation we will describe a possible way towards a Security Service Challenge spanning the Infrastructures coordinated by EGI and OSG, with the goal of assessing our readiness to manage a global incident affecting the EGI and OSG infrastructures.

One way to tackle this is to break down the main exercise into challenges addressing the components of a globally coordinated incident response, and to run these first before getting everything together to challenge the overall security situation. To accomplish this, we will develop a table top roleplay for the infrastructure CSIRTs; in this roleplay the CSIRTs will handle a ficticious incident spanning the infrastructures. In their response the CSIRTs should follow their existing policies and procedures, with an important outcome being insight into where potential conflicts in these may exist.

In addition, it is hoped that this exercise will show whether the information necessary to handle the incident is available to the infrastructure CSIRTs. The availability of this information, used in an abstract way in the tabletop exercise, will be tested in separate challenges with the involved entities.

One example of this is the information available at the Virtual Organisations, or resource centers, in particular in the logs of the various services used to access the resources offered by the infrastructure.

Once the parts of the overall incident response are known to work, the SSC would then address the connections between the IR components and should give a meaningful assessment of our capabilities to an incident spanning multiple infrastructures.

Finally, as a result from SSC-19.03, the importance of having the evaluation of the different actions taken as soon as possible was demonstrated. Ideally this would be made available within a matter of days after the SSC is over; in the presentation we will show how a near time evaluation can be achieved.

Primary authors: Dr CROOKS, David (UKRI STFC); Dr GABRIEL, Sven (Nikhef/EGI); Mr BRILLAULT, Vincent (CERN/EGI)

Co-authors: KRASOVEC, Barbara (Jozef Stefan Institute); KOURIL, Daniel (Masaryk University); Dr GROEP, David (Nikhef); Dr KELSEY, David (STFC-RAL); TEHERAN, Jeny (Fermi National Accelerator Laboratory); CAILLAT-VALLET, Laurent (IN2P3 Computing Center); STANFIELD, Mike (Indiana University); DIA, Nuno (LIP); SONS, Susan (Indiana University)

Presenter: Dr GABRIEL, Sven (Nikhef/EGI)

Session Classification: Network, Security, Infrastructure & Operations Session

Track Classification: Network, Security, Infrastructure & Operations