Annual Report 2016-2017

Margrete Raaum, Chair

Serge Droz
Kate Gagnon
Aaron Kaplan
Koichiro Komiyama
Derrick Scholl
Damir ‘Gaus’ Rajnovic
Thomas Schreck
Maarten Van Horenbeeck
Adli Wahid

FIRST Annual Report 2016-2017

Dear reader,

This is the first year that the Forum of Incident Response and Security Teams (FIRST) publishes an annual report. The goal of the Annual Report is to provide a short summary of the activities of FIRST during the last year. The report covers the time between our Annual Conference in Seoul, in June of 2016, through our conference in Puerto Rico, June of 2017.

This year was an exciting time for FIRST. We grew our membership to over 380 members, and now have members in 81 countries. Several new SIGs were launched and we had a large number of events across the world. In addition, we released the TLP and IEP standards and for the first time, released our trainings under a Creative Commons license.

This year, we also see a change of hands in the leadership of our organization. In 2017, I have reached my term limit as Chair. I will step down from this role and continue on as board member for the next two years. Incoming leadership are Thomas Schreck, our new Chair, and Damir 'Gaus' Rajnovic who continues on as our CFO. We've accomplished a lot over the last two years, and it is with pride that I can hand off the ongoing work. I trust that with them, our organization is in great hands and well positioned for future growth.

As always, our members are what makes FIRST tick. We'd like to thank them specifically for the time they have invested in our organization, and look forward to seeing where they will help bring us next.

Best regards,

Margrete Raaum
Chair, Forum of Incident Response and Security Teams

Table of contents

Organizational goals

Over the last few years, FIRST has focused its goals across three wide initiatives:

- During an incident, it is important that incident response teams have immediate contacts at their counterparts in the world, whether they manage the network where the attack originates, or support software, devices or systems which help defend against the attack. **We grow our membership to enable these relationships.**
- We ensure member teams have a similar understanding of the incident response world, enabling them to quickly build trust and cooperation across organizational and national boundaries. **We develop and maintain a services framework that defines typical CSIRT services, developing and providing training, and enabling working groups where teams can work together on hard problems.**
- We help teams automate where possible, enabling computers to do the heavy lifting, while human talent is inspired to solve the hard problems. **We develop standards, provide guidance on information sharing, and enable teams to share information and brainstorm at events.**

During the year, we have been working on a fourth major pillar in our work, which is in many ways new to us. FIRST has started investing some time educating non-CSIRT teams about the role of incident responders and our technical community. We do this by contributing technical expertise to Internet governance bodies and policy forums. We are not a policy maker and do not intend to be one. However, we heard from our membership that providing technical expertise and guidance on what our community of incident responders do is important to enable policy makers to be successful. We expect in future years this fourth major pillar will continue and become a bigger part of our mission and goals.

Major announcements and press

During the last year, FIRST made the following major announcements:

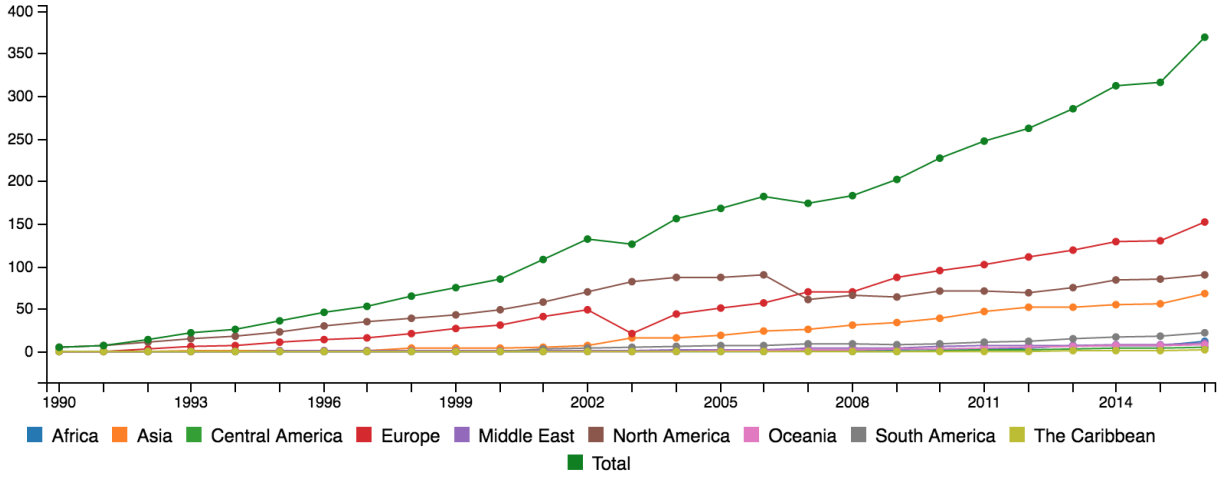
- On July 11th, 2016, did a public call for participants in a new Special Interest Group on Malware Analysis
- On August 11th, 2016, announced that the Fellowship program, which had brought 10 fellow teams into the FIRST community so far, will now be known as the Suguru Yamaguchi Fellowship Program, in memory of late Board member Suguru Yamaguchi
- On August 31st, 2016, announced the release of the inaugural version of the Traffic Light Protocol standard
- In September of 2016, published the first release of the Information Exchange Policy (IEP)
- On November 22nd of 2016, signed an agreement with LACNIC to improve incident response capability in Latin America and the Caribbean. In particular, FIRST and LACNIC will cooperate on organizing joint events
- On April 11th, 2017, signed an agreement with OASIS to cooperate and promote cybersecurity standardization, in particular on STIX and TAXII
- On April 18th, 2017, published twenty years of conference materials from our events on our public web site. This content is no longer gated to members
- On May 19th, 2017, released version 1.1. of the CSIRT Services Framework, incorporating feedback from the community
- On June 7th, 2017, released learning.first.org, an on-line, interactive training platform for our standards and technologies, as well as our incident response trainings
- On June 8th, 2017, released a draft Standard Policy for Public Input. This document will guide future standards development within FIRST, covering intellectual property rights, consensus building and public review processes
- On June 14th, 2017, released a draft Framework for Product Security Incident Response teams for public input
- On June 15th, 2017, announced signing a cooperation agreement with OIC-CERT and GÉANT, to cooperate more closely on training and membership

FIRST was highlighted in several media articles over the last year, including no less than 65 articles in the Korean press covering our annual conference. For the first time, FIRST organized a press briefing at the event which was attended by 20 Korean and Japanese journalists.

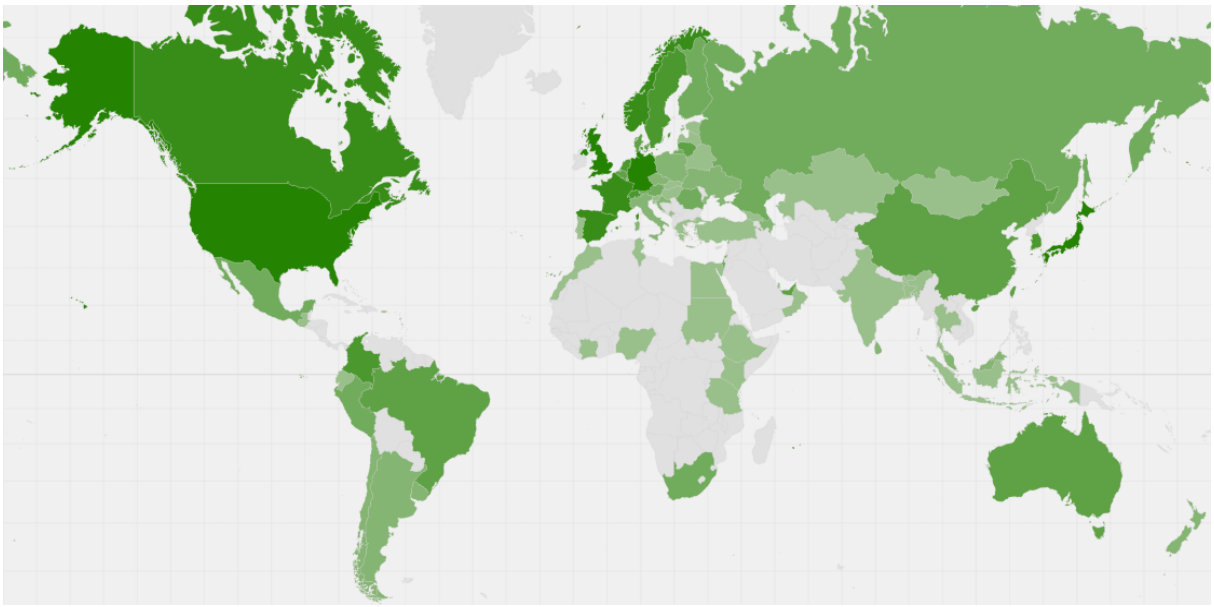
FIRST was also mentioned in an article in Forbes covering how global security experts have a difficult time immigrating to the United States. Board Member Maarten Van Horenbeeck published 2017 predictions in ITProPortal covering security issues over the next year. SCMagazine interviewed our former Chair, Margrete Raaum, about how we can encourage more women to join the IT sector and board member Katherine Gagnon was interviewed by YonHapNews in South Korea about her experience in security plus the risk of smart home and smart car threats. More articles covering FIRST can be found in the "In the News" section of our web site.

Organizational updates

Membership



FIRST saw healthy growth in 2016, with a total of 380 members by the end of the 2017 annual conference. Membership grew mostly in Europe and Asia. FIRST membership is also increasingly becoming international for we now have members in a total of 81 countries, compared to 77 last year.



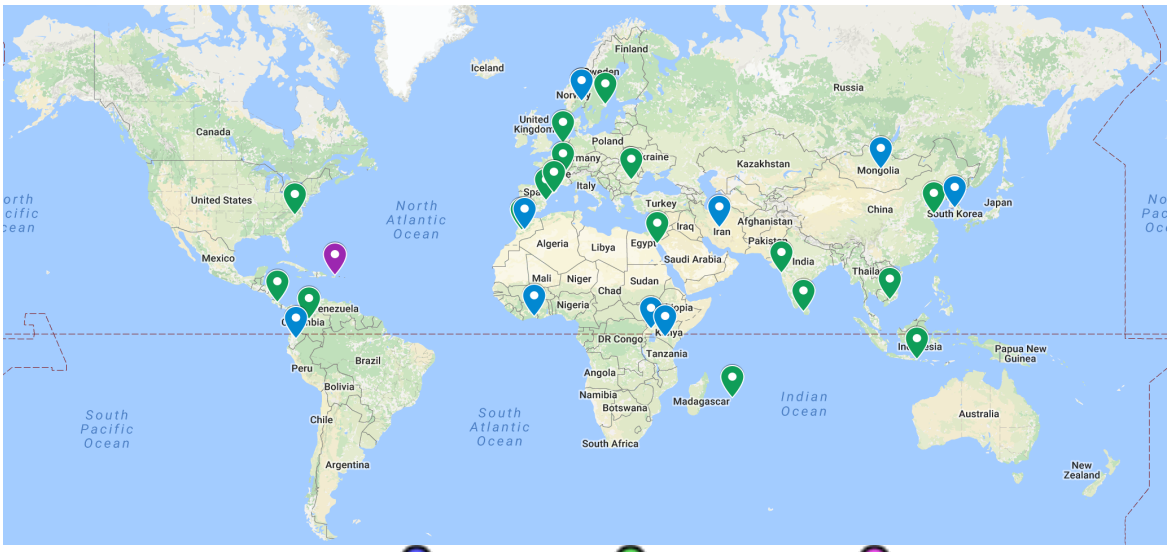
As Internet use grows across the world, there is an increased need to bring incident response teams from developing economies into our community. At the Seoul conference, keynote speaker Kilnam Choi challenged us not to rest until we have all countries on board.

The **Suguru Yamaguchi Fellowship Program** helps us towards this goal by enabling teams to join our community more readily. In 2016, four teams from Bangladesh, Myanmar, Cote d'Ivoire, and Ghana participated in the program while in 2017, teams from Vietnam, Panama, Ecuador and Moldova joined. The full roster of Fellowship teams is now 11 teams, though three teams have dropped from the program. Thus far, three teams has joined as a full member.

Read more about our membership at https://www.first.org/members/.

Suguru Yamaguchi Fellowship Program participants and Board Members, Seoul Conference 2016

Events



FIRST activity across the world: Training classes TC's and Symposia Annual conference 2017)

FIRST organized 3 Symposia, 17 Technical Colloquia and 7 trainings around the world. These events are opportunities not only to exchange ideas and know how, but also to grow trust and meet peers. In 2016 FIRST also published a site selection guideline to help us finding suitable and safe venues for our activities. Our events and training sessions would not be possible without volunteers, and we invite interested parties to contact us if interested in contributing.

Read more about our events at https://www.first.org/events/first.

Delegates at the FIRST Regional Symposium for the Arab and African regions, November 2016.

Training and Education

FIRST has recognized Training and Education as one of its priorities. In 2017 we published a draft of the PSIRT Services Framework and an updated version of the CSIRT Services Frameworks. These documents, developed by experts from the FIRST community, systematically describe the services delivered by teams. The services frameworks have attracted much more interest than we initially anticipated for they are used by other multinational organizations in various ways.

Thanks to a generous stipend from UK Foreign & Commonwealth Office for 2015/6 we were able to develop new basic training materials and a Fusion course. We have tested these materials in several trainings around the world and both have now been released under a creative commons license on our webpage. The feedback is very encouraging.

The CVSS SIG also created our first online course, available on our new learning.first.org platform.

A survey conducted in fall 2016 showed that our members would like to have courses on information collection and sharing, netflow, and log analysis. We currently are seeking funding to develop such course material.

Read more about our training and education program at https://www.first.org/education/.

FIRST Training: CSIRT Operations in NRENs in Abidjan, Côte d'Ivoire, April 2016

Special Interest Groups

FIRST organizes Special Interest Groups by request of membership, and provides them with support, such as web site infrastructure, a conference bridge, a Program Manager, and meeting space at our events.

During the year, the following new SIGs were implemented:

- **Malware Analysis:** The Malware Analysis SIG had existed for several years but was dormant. It was restarted in 2016 and has since published a list of references in Malware Analysis and is working on a Best Practices document describing how organizations typically conduct malware investigations.
- **Ethics SIG:** this SIG has as goal to develop a Code of Conduct for the FIRST membership to guide proper roles and expected behavior of CSIRTs.

Several SIGs published work efforts during the year, including the Vulnerability Coordination SIG, which worked with the National Telecommunications and Information Agency (NTIA) of the United States to publish a draft *Guidelines and Practices for Multi-Party Vulnerability Coordination* for public comment in late 2016. The Traffic Light Protocol and Information Exchange Policy SIGs also both published inaugural versions of their standards.

Read more about our Special Interest Groups at https://www.first.org/global/sigs/

Standards

FIRST supports the development of standards and maintains four different cybersecurity standards: Throughout the year, groups worked on:

- The **Common Vulnerability Scoring System (CVSS):** develops and maintains the CVSS standard, a robust and useful scoring system for IT vulnerabilities that allows organizations to prioritize them across their networks. CVSSv3 has also been published as an ITU recommendation in X.1521:2016. In the first half of 2017, FIRST released an interactive training "Mastering CVSSv3" through our learning platform.
- The **Traffic Light Protocol (TLP)**, a set of designations used to ensure a common expectation in audience for (non-automated) iterative sharing of sensitive information between entities. The initial version of this standard, building on the original TLP, was released in September of 2016.
- The **Information Exchange Policy (IEP)**, a framework for defining information exchange policy, and a set of common definitions for the most common sharing restrictions. It addresses information exchange challenges and promotes information exchange more broadly, primarily for machine automated communications. The first version of the standard was released in September of 2016.
- **Passive DNS exchange:** a common output format for Passive DNS servers. Released in 2015, this standard is made available as part of an IETF RFC, and is seeing continued development within the FIRST community.

In addition, FIRST continues to be represented as a sector member in the ITU as a standards body. FIRST also signed a Memorandum of Understanding with standards organization OASIS to permit closer cooperation on threat intelligence specifications such as STIX and TAXII.

Read more about our Special Interest Groups at https://www.first.org/standards.

Internet Governance and Policy

As a member of the Internet Technical Community, FIRST has engaged with policymakers and Internet governance bodies to provide technical expertise where appropriate. While FIRST does not engage in policymaking efforts, we do contribute to technical discussions contributing to the wider Internet governance debate. In particular, we educate policymakers and other stakeholder communities about the challenges of the Incident Response community.

During the last year:

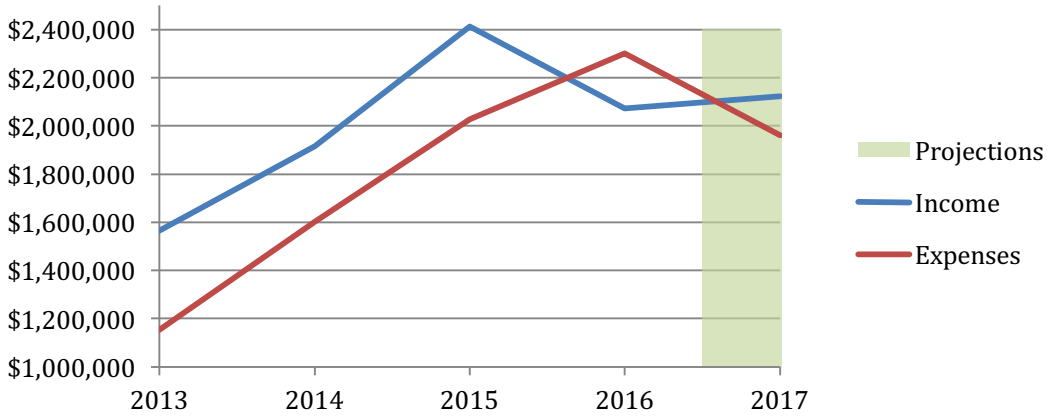
- FIRST members functioned as lead experts to the Best Practices Forum on Cybersecurity, organized by the Internet Governance Forum in Guadalajara, Mexico;
- Board member Serge Droz participated in the ICT4Peace Cybersecurity Policy and Diplomacy initiative in Vientiane, Laos;
- Board member Maarten Van Horenbeeck participated in a panel on challenges in international cooperation in Riyadh, Saudi Arabia, at the 2nd Annual International Cyber Security Conference, organized by the Saudi Arabian National Cyber Security Center.

Read more about our Internet governance and policy work at https://www.first.org/global/governance/

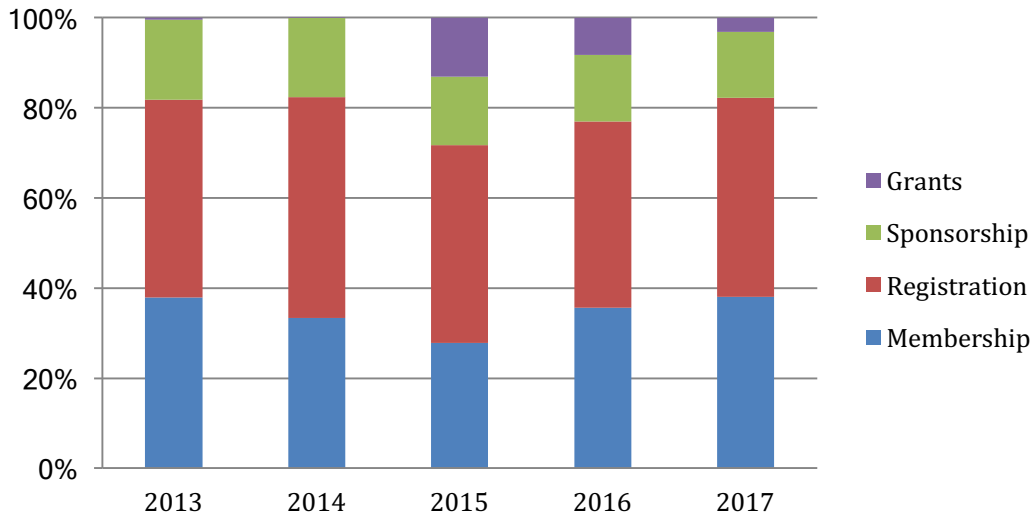
Board member Maarten Van Horenbeeck participates in a discussion on cybersecurity cooperation

Financials

In 2016, FIRST booked an overall loss of $283,976. This was projected in our budget for the year, and was mostly due to the expense of organizing our annual conference in Seoul. In addition, FIRST incurred expenses this year due to a migration effort of our technical infrastructure, which was overdue.



FIRST's income for 2017 was distributed across membership fees (36%), conference registration (45%) and sponsorship (17%). We did not obtain new grants during the timeframe covered by this report, though the final spending for a grant received in 2016 did extend until April 2017 earmarked for training development.



FIRST is a financially sound organization and a 501c3 non-profit incorporated in North Carolina, USA. Detailed financial information is made available through our members portal, or can be provided upon request to interested parties such as grantors and sponsors.

Infrastructure

During this year, FIRST heavily invested in infrastructure. The following significant changes were made as a result:

- FIRST moved most services to a new hosting provider selected through an RFP process to lower cost and increase abilities to manage our wide set of services;
- FIRST initiated implementation of an Association Management System. This was a recommendation from our 2015 audit, and will allow the Board and Secretariat to more effectively deal with our needs as a growing organization. The AMS will allow easy dashboarding of membership growth and permit a day-to-day view of the organization.
- FIRST deployed, with the support of CIRCL, a Malware Information Sharing Platform (MISP) instance operated by the Information Sharing Operations SIG.
- The web site was refreshed to make it easier to use from mobile devices. As part of the refresh, we moved to a Markdown based system managed through Git repositories. This ensures greater security as the site is dominantly static HTML and allows more parties to edit the site directly through Git rather than relying on our webmaster for minor changes.

The new FIRST web site with better support for mobile devices

https://www.first.org/
first-sec@first.org

Forum of Incident Response and Security Teams
PO Box 1187
Morrisville
North Carolina 27560-1187
United States of America