FIRST POST
Summer 2020
Bringing together Security and Incident Response teams from around the globe.

2020 AGM & ELECTION

By Serge Droz

The Annual General Meeting (AGM) is typically where FIRST members meet, where organizational updates are announced and where decisions are made about future operations. A required agenda item during the AGM is the election of five new Board of Directors that become vacant each year.

The current Board has consulted with our attorney, after we had to postpone the June conference due to COVID-19, and we were informed that an AGM and Election must take place to meet our obligations under the North Carolina law where FIRST is incorporated.

The election will take place online between 8th – 22nd July 2020. We have offered the option to e-vote for the past few years - the difference this year is that all primary team representatives will be provided with a link to the e-ballot to vote. There will be no other votes cast outside the online election. Every team primary representative will be able to vote and cannot pass proxy for election voting.

The AGM will be followed by a FIRST Members Update. This will include updates on financials, membership, activities/events and will include opportunity for members to ask questions. This session happens outside of but immediately following the AGM and will also be streamed and recorded for members. If you already have questions that you would like answered, please let us know, so we can prepare.

A FAQ can be found on the **FIRST Portal**. It is very important that your team's contact information and primary representative are up to date and you have FIRST Portal access to submit the required forms and ballot for the election. Some important upcoming dates:

- Call for Nominations Deadline – July 1, 2020 23:59 UTC
- Call for Proxy Deadlines – July 1, 2020 23:59 UTC
- Primary Team Representative Changes Frozen – July 1, 2020 23:59 UTC
- E-voting Opens – July 8, 2020 00:00 UTC
- E-voting Closes – July 22, 2020 23:59 UTC
- AGM – July 29, 2020 13:00 UTC
- FIRST Update – July 29, 2020 Directly following AGM

The Board made these decisions based on the best interest of FIRST in order to fulfill our legal obligations and hold a fair election. We thank you for your support in these challenging times. For any questions, feel free to reach out to me directly at **chair@first.org**.

Serge Droz, Chair, FIRST

2020 CONFERENCE UPDATE AND IMPACT OF COVID-19

by Derrick Scholl

The FIRST Annual Conference in Montreal has been rescheduled to the week of November 15-20, 2020. We are still working out the specifics and plan to share additional details on the format and program and reopen registration in the coming weeks.

We are very much aware of how challenging it is to prepare for an in-person event this year. First and foremost will always be the safety and comfort of our attendees, presenters, and staff.

Physical distancing plans

Our plan right now is to give ourselves the option for a best case scenario of a reduced attendance conference. To ensure the safety of participants, we plan to put in place a number of physical distancing measures including adequate spacing between seats, elimination of handshakes, increased use of technology to ensure seamless and fast registration, pre-packaged food to replace buffets, working with our venue partner to ensure enhanced frequent cleanings of conference rooms, wearing masks and so on.

We are also investigating the option of a virtual attendance for those who can't attend.

Program

We are in touch with our accepted speakers to gauge interest in attending/presenting in person vs. virtually. Once we have more details, we will update the program online. However, there is an increased risk of fewer tracks and cancellations so we will need to prepare for any scenario the best we can. We are working hard to make sure those that can attend have a great experience – even if it is a little different from previous years.

Travel precautions

Due to this uncertainty, our events team have provided some recommendations for you to consider when rebooking your travel:

- Start the planning process now. Talk to your managers about what tentative travel policies might look like in November.
- Research, understand, and apply for your visa (if applicable) as soon as agencies will allow it. Processing times may take longer than usual given the circumstances. Use this page for guidance on re-openings here: https://www.canada.ca/en/immigration-refugees-citizenship/services/visit-canada.html.
- Consider booking refundable/changeable airfare and travel insurance.
- Should the unfortunate happen, be prepared with details of your health insurance and best options for receiving care in Montreal (which may include a travel medical insurance policy). Please understand that health coverage varies greatly so it is the responsibility of each individual to know and manage their best options for (emergency) care abroad.
- If you are not planning to book and stay at the conference hotel (Fairmont The Queen Elizabeth), we encourage you to please read and understand booking terms and conditions as well as their safety procedures relating to COVID-19.
- If you are planning to book at the conference hotel (Fairmont The Queen Elizabeth), please know that our event organizers are working very closely with the hotel and will have all the pertinent information relating to the reservation process—from booking to arrival—available on the conference website in the upcoming weeks.

Alternative option

If travel restrictions remain in place, or if a great number of employers or attendees don't feel comfortable with the idea of traveling to an event where lots of people will be gathering, we must also consider that there's a very real possibility that we may not be able to hold an in-person event in November. So with this in mind, we're currently preparing for the option for the entire conference to be held online - we'll keep you regularly updated in the next few months.

Please continue to check the **conference website** for additional procedure updates and safety guidelines over the upcoming weeks.

We hope to see many of you this November in Montreal if all goes well!

Derrick Scholl
FIRST Board of Directors
2020 Conference Chair

FIRST 2020 CTI SYMPOSIUM IN SWITZERLAND MOVED ONLINE

Our 2020 CTI Symposium which was due to take place in March in the beautiful town of Zürich, Switzerland was moved online after COVID-19 became a global health risk for our participants. Speakers and the participants were keen for the event to go ahead so rather than cancel the Symposium completely we worked with our event organisers to create a valuable online event. This was a first for us.

We worked with our events organization to build a two week event featuring two talks per day that suited all participants across many time zones. This worked out well, although those in Europe had to watch the talks in the evening and participants from the Asia-Pacific region had to watch it late at night. While this wasn't entirely convenient it was the best solution at the time.

With great content and interested participants we demonstrated that you can have a high quality conference online. But there were also challenges, in particular speakers who missed the interaction of a live audience. We also realized that humans are social beings, and we all missed the time outside the talks to build relationships and network. We hope that face to face meetings return soon.

FIRST members can watch the Symposium's presentations online through our new Portal **here**.

FIRST TO REVIEW THE TRAFFIC LIGHT PROTOCOL STANDARD TO INCREASE GLOBAL ADOPTION

We're inviting participants for the next round of reviews to standardize the Traffic Light Protocol (TLP). Targeted at CSIRTs, PSIRTs, operational trust communities, information sharing analysis organizations, government agencies, and private researchers, the original TLP was created to encourage information sharing among public and private sector security professionals in the United Kingdom. We recognized the need to develop it further

Now, a new refinement round starts, that should lead to TLP being formally adopted as a FIRST Standard.

Thomas Millar, TLP-SIG chair said: "These changes will not alter the way in which TLP is currently being used by hundreds of security teams around the world, but it will help teams to interpret TLP more easily. The increased transparency of the FIRST Standards process

first-sec@first.org

FIRST UPDATES COORDINATION PRINCIPLES FOR MULTI-PARTY VULNERABILITY COORDINATION AND DISCLOSURE

As part of our mission to encourage global coordination and a global language, we have released an updated Guidelines for **Multi-Party Vulnerability Coordination and Disclosure** version 1.1. The Guidelines can improve coordination and communications across different stakeholders during a vulnerability disclosure. They provide best practices, policy and processes for reporting any issues across multiple vendors and areas targeted at vulnerabilities that have the potential to affect a wide range of vendors and technologies at the same time.

The Guidance includes:

- Establish a strong foundation of processes and relationships
- Maintain clear and consistent communications
- Build and maintain trust
- Minimize exposure for stakeholders
- Respond quickly to early disclosure
- Use coordinators when appropriate
- Multi-Party Disclosure Use Cases

You can find the new Guidelines **here**

"As software development becomes more complex and connected to supply chains, coordinated vulnerability disclosure practices need to evolve. The updated Guidelines are a step in that evolution, deriving guidance and principles from practical use cases."

Art Manion, Vulnerability Analysis Technical Manager, CERT Coordination Center

FIRST AND MITRE ENGENUITY PARTNER TO EXPAND THE GLOBAL UNDERSTANDING OF ADVERSARY BEHAVIORS

Our readers will be aware of the MITRE ATT&CK framework - the globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. Rich Struse of MITRE has presented on the framework at the last couple of conferences and at the CTI event in London last year. It has received wide praise as it enables a common language and taxonomy that we can use to work together and better defend our systems.

MITRE have built a privately funded research and development centre to take this work forward - the MITRE Engenuity Center for Threat Informed Defense. The goal of this center is to advance a shared understanding of cyber adversaries, their tradecraft, and technology - and then develop ways to prevent, detect or mitigate attacks. The Center enables collaborative research and development that results in technologies and methodologies available to all that strengthen our collective defences.

The centre has brought together a number of partners including the finance, health, technology and information sharing sectors and is still growing.

ATT&CK®

FIRST has now joined as a non-profit participant. This will enable us to work with the centre to identify the most critical challenges in threat informed defence and solve them collaboratively as well as sustain and advance the ATT&CK ecosystem. We can bring the practical, real-world, experience of our membership to the table.

For more details on the center see **here** or email Chris Gibson (**chris@first.org**)

A shared understanding of cyber adversaries, their tradecraft, and technology.

MORE NEW PARTNERSHIPS FORGED TO MAKE THE INTERNET SAFE FOR EVERYONE

FIRST is committed to making the internet a safe place for everyone across the world. With this in mind we have chosen to support a number of projects in 2020 that are focused on similar goals. These include Cyber4Healthcare and the Work from Home Campaign.

Cyber4Healthcare, initiated by the Geneva based Cyber Peace Institute, connects health-care organizations in need of cybersecurity advice with reputable organizations willing to offer cybersecurity assistance services free of charge. The free service is for hospitals, care facilities, clinics, labs, and clinicians, as well as pharmaceutical, life sciences, and medical device companies that are providing, researching, developing, and manufacturing COVID-related treatments. It is also applicable to non-governmental organizations (NGOs), and international non-governmental organizations (INGOs) working to combat COVID-19. For more information, please visit their webpage - **www.cyber4healthcare.org.**

Work from Home Campaign. Secure Your Business. This campaign, kicked off by our partners from the Global Cyber Alliance, is focused on shoring up the defenses of a newly remote workforce due to the COVID-19 pandemic. Many businesses have been forced to move their day-to-day operations from offices to their employees' homes, which creates new security risks for businesses, their customers, and employees. The campaign, **https://work-fromhome.globalcyberalliance.org** provides clear, actionable guidance including links to tools and step-by-step instructions that can be used by companies and employees working remotely to take immediate action and put better security in place at home.

VIRTUAL SITE VISITS CURRENTLY AVAILABLE FOR NEW APPLICANTS

During our April 2020 meeting, the Board voted to temporarily grant a general exception, from the requirement for a physical site visit for new membership applicants. The Board made this decision due to restrictions caused by COVID-19 and to ensure that membership applications may continue, however, we have requested higher diligence by sponsors. Virtual site visits can now be leveraged by sponsoring teams until further notice. Mandatory and recommended items noted in the FIRST Site Visit Guide need to be still reviewed, discussed and noted in the sponsor's site visit report. However, these items may now be reviewed/discussed in a webinar format. In no way shall this exception set a precedent for future membership process changes and quality control methods will remain in place. Guidelines for virtual site visits can be found **here** and below:

- The sponsor should have prior relationship/working knowledge of the team they are sponsoring. A virtual site visit may not be accepted if the teams have not met in person previously or haven't had a prior working relationship.

- Conduct the site visit over several hours/sessions. Please don't rush through the checklist. We recommend dividing the discussions over several sessions. You may also review in a shared document format where comments can be documented and revisited for a thorough review.

- Focus on what is important: confidentiality of information, communication methods and meeting the team.

- Meet the full team. It is important to involve more than just the team rep/leader in the site visit. A portion of the virtual visit should involve meeting the majority (if not all) team members.

- Physical security – Since you cannot be onsite, we require a detailed explanation of the physical security and facilities and equipment discussed.

The Site Visit Checklist has also been modified to include some considerations for virtual site visits to acknowledge the following:

- A physical site visit was not possible at this time but the team has met with the team/members of the team in person on other occasions (recommended).

- If the sponsor has visited one or more physical locations of the company on another occasion previously (recommended).

- Request details on when the virtual site visit took place, duration and who was present and note if the virtual site visit took place over several occasions or a single session (mandatory)

We ask that all sponsoring teams remember that it is your responsibility to attest that the applying team satisfies the minimum requirements for FIRST membership and that you have an understanding with the way the candidate team operates. If you do not feel completely confident that your recommendation can be established with a virtual meeting (either before or after you conduct the virtual visit with the team) – we recommend that application remain on hold and that you reschedule an in person visit once the current restrictions are lifted.

For any questions or concerns, please contact the FIRST Secretariat at first-sec@first.org.

Opinion

CRITICAL VPN VULNERABILITIES SHOW THE NEED FOR PROACTIVE RISK SCANNING

By Matthijs Koot

Last year, researchers discovered and reported critical vulnerabilities in various high-end VPN products. Attackers have been known to exploit these vulnerabilities to access data and systems that should be restricted to legitimate VPN users. Organizations with unpatched VPN systems are exposed to the risk of ransomware, sabotage, and corporate or state-level espionage.

In early 2019, the VPN vendors released patches to fix vulnerabilities. In August 2019, more details about these vulnerabilities became publicly known. I was seriously concerned about possible real-life consequences of abuse of unpatched systems and decided to start unsolicited internet scanning to detect and report vulnerable VPN servers in the Netherlands.

The outcome of my research was outright shocking. Just one of the affected VPN products had over 500 unpatched systems linked to healthcare organizations, our government, financial industry, defense industry, aerospace industry, petrochemical industry, multinationals, harbor and transport organizations, education and IT providers (including some IT security providers). In many cases the vulnerable VPN system was a production system.

In early October 2019, both the National Security Agency and the Government Communications Headquarters released public warnings that Advanced Persistent Threat groups were actively exploiting VPN vulnerabilities around the globe. Similar warnings have been repeated in 2020 due to bad actors abusing VPN systems that are still unpatched, a year after patches were released. This is borderline insane given what's at stake. It also proves that the risks have manifested in practice: it is not about theoretical risks or fear, uncertainty or doubt, we're talking about real and practical risks.

Societies as a whole have a problem regarding patching and low awareness around patching and risks as a whole. Hence, we need to think about possible additional actions.

One way forward is to start holding vendors accountable for preventable vulnerabilities, but that is a complicated legal and political process. As long as critical vulnerabilities are found in internet-facing products, unsolicited internet scanning may help prevent abuse. A large part of the international CERT community appreciated the information they were given: it was actionable intelligence that was often missing in paid threat intelligence feeds they're subscribed to

After I completed the scanning for vulnerable VPNs, I joined the non-profit organization Dutch Institute for Vulnerability Disclosure (**DIVD**) as a volunteer researcher. DIVD performs ad-hoc internet scans to detect vulnerable systems and disseminate information to system owners and/or via national and international CERT channels.

Going forward, I would like to see a discussion in CERT realms on whether CERTs/CSIRTs can become (more) involved in unsolicited, proactive scanning of constituents regarding critical and remotely exploitable vulnerabilities. On the one hand, CERTs have an existing trust context with their constituent organizations and may know which person(s) to contact to get things fixed. On the other hand, each vulnerability is different and may require a new test method. That requires specialized technical knowledge and tradecraft, which may require cooperation between CERTs globally.

Unsolicited scanning has ethical, legal, organizational and technical aspects, but whatever the hurdles are, I strongly urge that we break with passivity and fear. Certainly when it comes to vulnerabilities at healthcare and educational organizations, such scanning truly helps protect the public interest.

Interested readers may read more in this Open Access publication:
Matthijs Koot. 2020. Field Note on CVE-2019-11510: Pulse Connect Secure SSL-VPN in the Netherlands. Digital Threats: Research and Practice 1, 2, Article 13 (May 2020), 7 pages. DOI: **here**

ISO AND STANDARDS UPDATE

While creating standards are not an incident responder's favourite pastime, they are nevertheless a very important element to securing the global internet. ISO standards in particular can have a big impact on our work. Standards help define a common vocabulary across our industry and help us to prevent misunderstandings. The process of creating a standard can be long and cumbersome at times but it forces participants to argue on the finer points of an issue. During the process we usually find a good consensus among participants - this journey can be just as important as the end result.

We are therefore very pleased that Shawn Richardson, from Nvidia, will support our engagement with ISO. Shawn is a very active member of FIRST and brings many years experience of working on standards. Your contribution is vital so if you are interested in contributing to our next round of ISO standardization please reach out to Damir Rajnovic **gaus@first.org** or Shawn Richardson **srichardson@nvidia.com**.

NEW BREACH WORKSHOP MATERIALS AVAILABLE

We reported on our successful new Breach Workshops conducted at the Fiji Symposium for Pacific Island nations in a previous issue of FIRST Post. The materials, created by Adli Wahid, Maarten van Horenbeeck and Serge Droz have now been published on our **website**.

Supported by the Australian DFAT, we hired a professional designer, who worked with our Chair to create vastly improved workshop materials this Spring. We took this opportunity to not only improve the design, but also the Breach Workshop training materials. The result was more attractive guidance and a more effective workshop. We are planning to extend this series with more scenarios.

ethicsfIRST

A NEW INITIATIVE TO BUILD TRUST

One of the most important elements for a successful incident response is trust. Building trust is hard and maintaining it takes constant effort. The Ethics SIG has been working for several years to create a Code of Ethics for incident response and security teams. It is applicable to all current and potential practitioners, instructors, students, influencers, and anyone who uses computing technology in an impactful way. Formulated as duties, these principles guide incident responders to identify the appropriate solutions to challenges in their work.

The code recognizes that often there are dilemmas, and encourages teams to find the best solution while considering their constituents and the public good. Please see **here**.

The Ethics SIG is looking for examples that could be analyzed with this code in mind. If you have an interesting, public, real world case, please contact us at **ethics-sig@first.org** for consideration.

FIRST INFRASTRUCTURE UPDATE
Portal & SSO

In April, FIRST released a new Portal and Single Sign-On (SSO) platform for use by team representatives, members, liaisons, collaborators and event attendees. The solution is approaching nearly a thousand users and provides a single point of access into all FIRST services and private resources. It replaces the use of X.509 certificates with strong passwords and multi-factor authentication options including: OTP, U2F, and Mobile App.

Members are now able to manage their profiles, access key FIRST resources including the directory, MISP, Wiki, and more from Portal. Representatives are able to manage their team profiles and rosters, perform AGM related tasks, and view and pay their dues invoices.

The Infrastructure team has more updates planned, including:

- Improved integration with National CSIRT teams & Fellowship participants
- Functionality for SIG participation and management
- Integration with the FIRST learning platform

Slack

In April FIRST made Slack workspace available to all members. This is an SSO-enabled service with channels in place for SIGs, events, and other specific topics of interest to the community. Access to FIRST Slack is available from within **Portal**.

"As our organization keeps growing this is an important milestone. Thanks to the time and effort spent by board member Dave Schwartzburg implementing the SSO solution we now have a solid foundation to add value services for our members."

Serge Droz, Chair

Thanks for reading!

Remember to follow us on our social media channels Facebook,
witter and LinkedIn for regular updates!