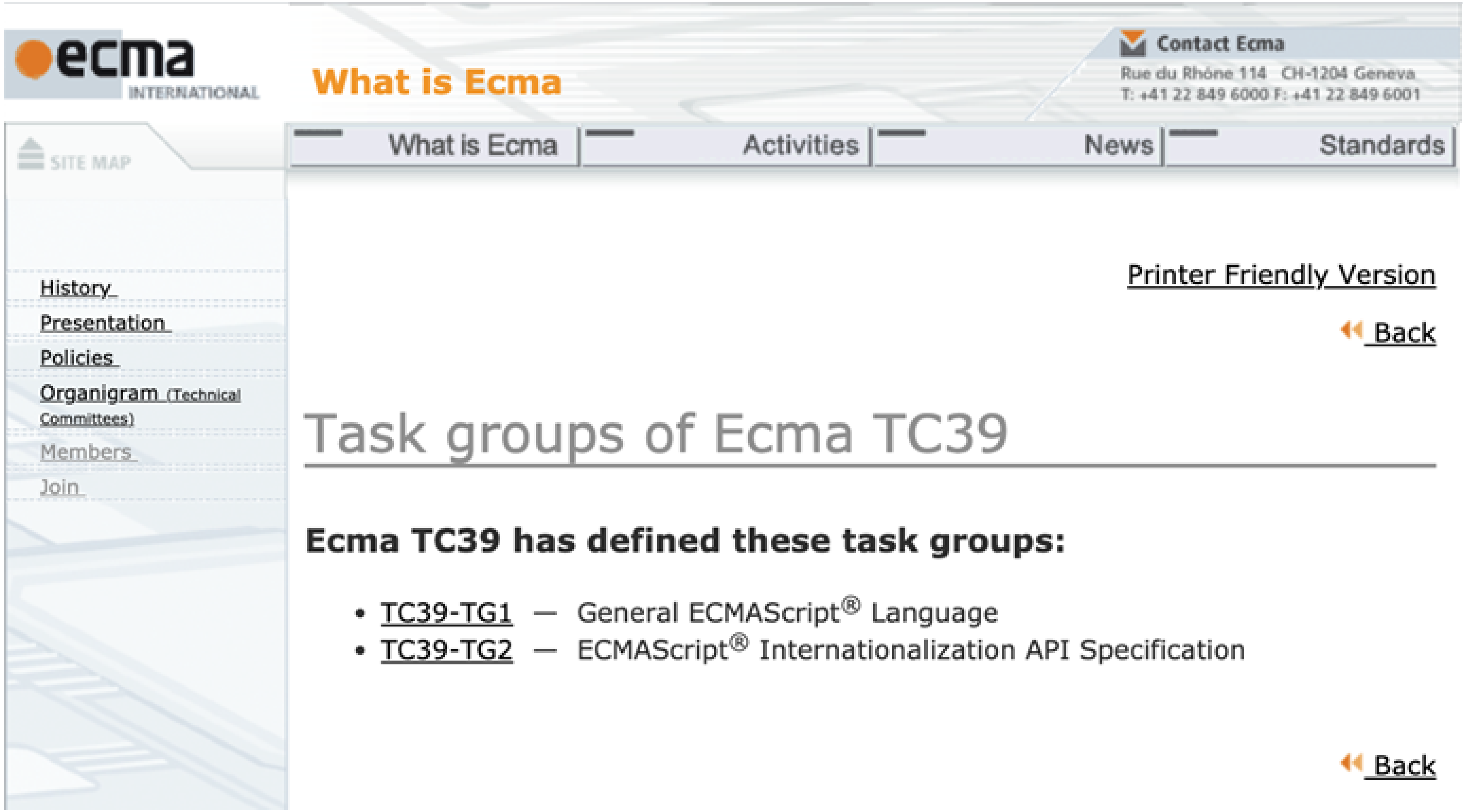
Chartering a Security Task Group

Michael Ficarra

TC39 · January 2021

https://github.com/tc39/Reflector/issues/313



Rue du Rhône 114 CH-1204 Geneva
T: +41 22 849 6000 F: +41 22 849 6001

Task groups of Ecma TC39

Ecma TC39 has defined these task groups:

- TC39-TG1 — General ECMAScript® Language
- TC39-TG2 — ECMAScript® Internationalization API Specification

https://www.ecma-international.org/memento/tc39-tgs.htm

Proposed Mission / Scope

1. assess the security impacts of proposals to TC39
   - designate security reviewers for proposals that advance to stage 2
2. produce documentation on the JavaScript security model
3. introduce proposals that will help developers create secure programs
4. recommend a committee response to privately-disclosed security issues
   - a la Spectre/Meltdown
5. maintain best practices or recommendations for writing secure programs
6. monitor the changing threat landscape for popular embeddings

Explicitly Not in Scope

Note: these are not in scope for TG output, though that does not prohibit the TG from considering/discussing them

- ECMAScript subsets or ECMAScript-derived languages, such as
    - StrongScript
    - Jessie
    - TypeScript
    - ActionScript
    - JSX
- the origin-based security model of the web

Example Early High-Level Agenda

Note: this is only an example; the final agenda will be set by the chair group

- understand and document adversarial domains in which JS is currently and commonly used, such as
  - mixed origin scripts on a web page
  - contracts / blockchain
- understand and document how JS is used today to write secure programs, such as
  - patterns / strategies
  - frameworks
  - tooling
- agree upon and document language invariants that can be relied upon for building secure programs
- collect and report on noteworthy implementation defects that have led to security issues
- document language features that are commonly the cause of security bugs, for whatever reason, such as
  - __proto__ accessors (accidental use in user code)
  - typed arrays with detached buffers (implementation errors)
  - mapped arguments objects (breaking assumed invariants)
  - direct eval (unnecessary use in user code)

Proposed Roles and Their Responsibilities

- Chair (Group)
  - Prioritisation of TG agenda
  - Management, organisation, communications
  - Meeting scheduling
  - Scope refinement
- Speaker
  - Create and deliver presentations to TG1
- Secretary
  - Ensure that the output of the TG is recorded and published for public consumption (as appropriate)

Example Process

Note: this is only an example; the final process will be set by the chair group

- Monthly meetings
  - iff the agenda is populated in advance (10 days?)
  - duration TBD at first meeting (3 hours?)
  - notes published to TC39/notes
- GitHub Discussions for communication outside meetings
- Regular status updates at TG1 meetings
- Yearly selection of leadership positions, coinciding with the TG1 election
- Deference to TG1 on all matters, whenever they feel the need to intervene

Participation Interest

- Shape Security, part of F5 Networks
- Dan Finlay (**@danfinlay**), MetaMask, part of ConsenSys
- Bradley Farias (**@bmeck**), GoDaddy Inc.
- Mark S. Miller (**@erights**), Agoric (**@Agoric**)
- Jordan Harband (**@ljharb**)
- Chengzhong Wu (**@legendecas**), Alibaba
- Yulia Startsev (**@codehag**), Mozilla
- Richard Gibson (**@gibson042**)
- Daniel Ehrenberg (**@littledan**), Igalia
- Caridy Patiño (**@caridy**), Salesforce
- Leo Balter (**@leobalter**), Salesforce
- Peter Hoddie (**@phoddie**), Moddable
- Shu-yu Guo (**@syg**), Google

What am I asking for us to agree to today?

1. TC39 consensus to sanction the creation of a TG with the scope and roles proposed herein.
2. TC39 chairs to prescribe a process for selecting TG leadership.