Ushahidi

www.ushahidi.com
info@ushahidi.com

US:
PO Box 782208
Orlando FL 32878-220
KENYA:
P.O. Box 58275-00200
Nairobi, Kenya

Security Update Q3 2012

Ushahidi has been tackling the issue of security with a two pronged approach. Technical Security and implementation best practices, particularly in Crisis Mapping. The effort is ongoing, these updates summarize what is currently in play.

1. A security policy aimed at informing the world about Ushahidi's stance towards security within the software is being drafted. It includes:

- The Ushahidi Security working group that has been at it since early this year. Information is tracked publicly on the wiki https://wiki.ushahidi.com/display/WIKI/Security+Working+Group

- The process for reporting security bugs. This is outlined on wiki pages (https://wiki.ushahidi.com/display/WIKI/Security+Best+Practices) as well as http://www.ushahidi.com/security.
- How to find out about security vulnerabilities that have been patched and information on the security patch process. This information is released immediately on both the main Ushahidi blog and the special http://www.ushahidi.com/security which Ushahidi has maintained since 2011. The overarching guideline being "While we try to create great software, the old adage applied: **Sometimes there will be bugs; we will fix them and advise you."**
- A complement to Crowdmap's Terms of Service as delineated on https://crowdmap.com/mhi/legal

2. A security policy aimed at users of the software and how they can/should lock down the application. This would be both technical and non-technical. It would provide guidance such as choosing strong passwords, properly configuring the web server and host systems, regularly applying updates and patches, etc. This is still a work in progress with the Security Working Group, but in the meantime, we actively provide information about best practices. The uses of the platform and geographical spread are varied. These are articulated publicly on the wiki and on the security blog. A redesign of the homepage and community site will incorporate these links more effectively than is the case right now.

To be done Q3-Q4 2012: Incorporate the humanitarian/human rights best practices/lessons learned. This will be done in consultation with ICRC. Many thanks to Dr. Sally Chin Ushahidi board member for engaging on this on Ushahidi's behalf.

More Context: ICRC produced a document in late 2009 setting out professional standards for "protection" (ie protecting civilians in armed conflict) including managing sensitive data. Our team representative (Rob Baker) will attend the upcoming ICRC sponsored event to review best practices in privacy and security.

Ushahidi's partners in the online security world are also supporting our efforts. We are in preliminary discussions with Tactical Tech to provide a webinar for our community about online security. Access Now and Rogue Genius have included Ushahidi in the Humanitarian Hack Box (http://roguegenius.com/hhb). This is a security review contest requesting that all security bugs be reported to that team. We have requested that all items also be shared with Ushahidi as per our updated security review process as listed on ushahidi.com/security.

What was realised was that this was getting outdated given all the new developments within crowdsourcing, crisismapping etc. Late 2011, an advisory committee to help redraft some of the chapters and there is now this consultation happening later this month with the crisismapping, satellites etc community to discuss how we all deal with sensitive data, both from a "technological solutions" standpoint as well as from a "principles" standpoint (ie, what are we striving for when we deal with sensitive data and the populations we work with). Output of the discussions will be a document on the Ushahidi blog and websites explaining our approach to safety and security, much in the vein of other media companies.

Ushahidi does not have a dedicated fully skilled info-sec consultant or staff member at our disposal. In the past, security experts at Internews and Rogue Genius have provided us with feedback on security issues. We have also reached out and continue discussions with The Citizen Lab to find ways to work together. This has been an informal "in-kind" action. The Security Working Group will review items and we can request guidance from our community. However, resolved security issues are critical to the safety of our users and the team continues to act as fast as possible to address issues that come to light, provide patches and communicate to the community. In the meantime, Robbie Mackay an experienced Ushahidi developer will be the main point of contact on all technical security questions Robbie@ushahidi.com and security@ushahidi.com. Non-tech and community point of contact is Heather Leson hleson@ushahidi.com.