FIRe: Firefox for Computer Security Incident Reporting and Coordination

Ashutosh Bahuguna*

Abstract

Information Security breaches are on the increase and adversaries are regularly coming up with new tools and techniques to compromise the information infrastructure. Effective incident information sharing and coordination during incident resolution is crucial for thwarting the cyber attack and protecting the critical assets of organization and nation. It is observed from the current means and methods employed by various national Computer Security Incident Response Teams (CSIRT) and Information Sharing and Analysis Centers (ISAC) that there is need for improvement in the incident reporting and coordination means & methods, relaying only few available means like unsecured email communication is insufficient in countering cyber attacks. FIRe (Firefox for Incident Reporting) is developed to provide reporting organization, a single window solution for incident reporting & coordination activities with CSIRTs (National & Sectoral) during incident resolution process. FIRe is a customized Firefox browser with extensions developed to enable the organizations to share the incident information in standardize format with the national and/or sectoral CSIRTs. FIRe provides the functionalities to communicate & coordinate during the incident resolution. FIRe also integrated tools for secure communication, sensitive information labeling, real time interaction with handler & analyst and database of stakeholder point of contacts. Operational testing of FIRe is planned in upcoming national cyber security exercise 2015 to be conducted by Indian Computer Emergency Response Team (CERT-In). Learning's of exercise and feedback of participating organizations with respect to FIRe will be used for improving the tool.

Keywords: Computer Emergency Response Team (CERT); Computer Security Incident Response Team (CSIRT); Incident Reporting; Incident Handling; Incident Coordination; Indicators of Compromise (IOC)

Introduction

A security incident is defined as an adverse event in an information system and/or network that pose a threat to computer or network security. In other words, an incident is any event that causes, or may cause a breach of information security in respect of availability, integrity and confidentiality. Examples of such incidents could be unauthorized access to information system, disruption of data, denial of services/ availability, misuse of system resources, malwaresand others. Large scale cyber incidents may overwhelm government, public and private sector resources and services by disrupting functioning of critical information systems. Complications from disruptions of the magnitude may threaten lives, economy and national security. Rapid identification, incident information exchange and coordinated response can mitigate the damage caused by malicious cyberspace activity.

A significant cyber incident requires increased national and/or sectoral coordination. Study of different incident reporting and coordination means & methods adopted by CSIRTs worldwide reveals that there is lack of standardize formats, channels & methods, (to) report the incidents to CSIRT, (for) incident information exchange with CSIRTs & stakeholders and (for) coordination with CSIRT during incident resolution. It is also observed that there is only few instances where means for real time coordination for incident resolution is implemented. It comes finally to regional coordination bodies or national CSIRT to enable sectoral CSIRTs and organizations under their purview for improved incident reporting and coordination activities.

Ashutosh Bahuguna*
Scientist, Department of Electronics & IT,
Ministry of Communication & IT Electronics
Niketan, 6-CGO Complex, New Delhi-110003

FIRe (Firefox for Incident Reporting), an extended Firefox browser is developed with objective to standardize and enhance the incident reporting and coordination activities, it provides features for secure email communication, web-form based incident reporting, Instant messaging for coordination during incident resolution, information sensitivity labeling, access to centralized point of contact database of relevant stakeholders and sharing of Indicators of compromise (IoC). In summary, FIReis a tool to enable reporting party for better coordination & communication with national or/and sectoral CSIRTs during incident resolution process. There is notable effort by European Union Agency for Network and Information Security (ENISA) [1] in standardization of incident reporting across European union. ENISA also developed a tool Cyber Incident Reporting and Analysis System (CIRAS) [2][3], as per Article 13a: guidelines for incident reporting [2][3], for online incident reporting to replaces the electronics forms email exchange in incident reporting. FIRe is not only a incident reporting system but a tool with purpose of improving coordination & communication in handling cyber attacks.

This paper discuss need for improvement in incident reporting & coordination means & methods, objectives & features of FIRe tool and operational testing of FIRe in exercise scenarios. Study of implemented means & mediums by various national CSIRTs for facilitating coordination & communications between reporting entities and national CSIRT are also presented in this paper. The rest of the paper is organized as follows. Section 2 is about need and challenges of Computer Security Incidents Reporting. Section 3 discuss current computer security incident reporting practices and solutions at various national CERTs/CSIRT. In Section 4 FIRe functionality details are provided. Section 5 is about operational testing of FIRe in upcoming cyber security exercise. Finally section 6 concludes the paper with future roadmap for FIRe.

Computer Security Incidents Reporting

National and sectoral CSIRTs also known as Computer Emergency Response Teams (CERTs) are the national or sectoral nodal agencies for responding to the cyber security incidents [4]. National/Sectoral CSIRTs are using multiple channels for gathering the information related to the incidents impacting cyberspace under their purview. By reporting computer security incidents to CSIRTs, the organizations and users receive coordination with other entities & technical assistance in timely resolving of incidents. This also help national/sectoral CSIRTs to correlate the incidents thus reported and analyze them; draw inferences;

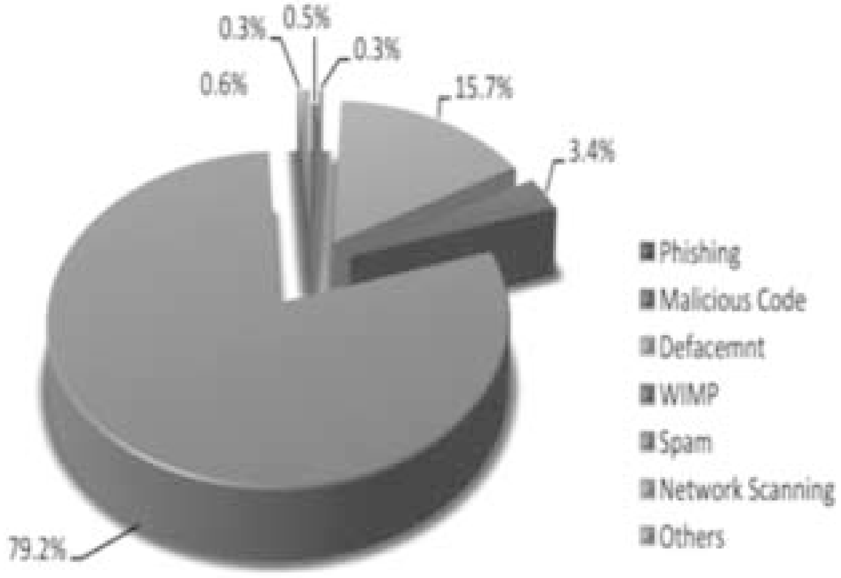


Figure 1. Cyber Intrusion During February, 2014.

disseminate up-to-date information and develop effective security guidelines to prevent occurrence of the incidents in future. Incident reporting need to be encouraged and supported by effective means of reporting & coordination tools and platforms.

CSIRTs are handling incidents reported and also monitoring the different sources for the incident information. Figure 1 is the breakup of incident reported & tracked by CERT-In in month of February, 2014 (Public Report: Monthly_report_CERT-In_Feb_2014) [5]. Most of the incidents in category Malicious code, Spam, Website Intrusion & Malware Propagation (WIMP) and defacement are tracked from various different sources. Study of the "incidents reported" and "incidents tracked" from other sources infer that large number of incidents (more than 70% percentage of incidents) remains unreported because of various possible reasons to organizations or users like lack of trust, lack of clarity and standard operating procedures for sharing information with external parties, reputation issues and others.

Trust of community on National and sectoral CSIRTs is vital for incident reporting and information sharing to CSIRT. Many organizations consider information sharing to external organizations as damaging to themselves, trusted CSIRTs (national and sectoral) are only hope for organizations to have help in incident resolution without any risk of damage to reporting party [6]. Organization or user reluctant to share incident information due to the confidentiality of data, legal and policy issues [7], reputation of organization, lack of trust or unwillingness to share data should be encouraged to share Indicators of Compromise (IoC) [8] instead of complete event data. Effectiveness of response actions of national CSIRT, for defending against cyber attacks, fundamentally depends upon percentage of incidents reported and tracked by CSIRT. To reduce the figure of unreported incidents, CSIRTs community need to focus on encouraging incident reporting & information exchange by developing and implementing the effective solutions for supporting communication & coordination activities during incident resolution. Streamlining the incident reporting process by standardization of incident data and incident reporting meanswould also improve operational efficiency of the CSIRT [9].

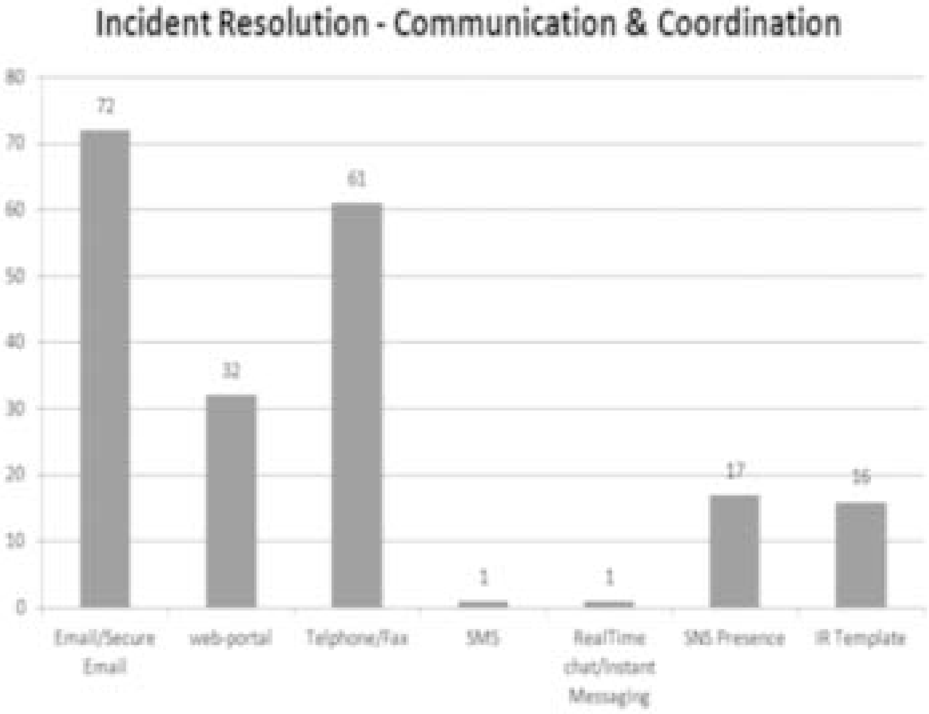


Figure 2. Incident Reporting and Coordination Solutions

Computer Security Incident Reporting Practices And Solutions

This section presents the main findings of the study on incident reporting & coordination means implemented by various national CSIRTs.Figure 2 presents result of the study, results are based on study of communication & coordination methods of 82 national and regional CSIRT [10]. Web-portals for incident reporting and incident reporting template (IR template) are efforts to enable the users to report the incident with required useful information about the incident, however these methods are not widely implemented. Among 82 CSIRTs, 17 CSIRTs are using social networking sites (SNS) like Twitter, LinkedIn and Facebook as a channel for interaction, which is again not a significant figure.

It is noteworthy that today also email and telephone/ fax are the main categories of communication channels in use followed by web-portals for incident reporting. There is a need of effective solution for enabling standardized incident reporting, real time interaction, information exchange & coordination activities. Real time communication & coordination enable analyst-to-analyst level interaction, rapid exchange of ideas & technical details and enhance trust & willingness for information sharing with external entities and national CSIRT, surprisingly only one CSIRT implemented the real time coordination solution for incident resolution & Short Message Service (SMS) based incident reporting. Looking at complex nature of current cyber security threat landscape, it is require to develop effective mechanism & means for incident reporting, communication & coordination activities during incident resolution and tools for supporting these activities.

Fire (Firefox For Incident Reporting)

FIRe is a customized Mozilla Firefox [11] browser which includes extensions for supporting incident reporting & incident resolution activities. Supporting server side applications like incident database, Internet Relay Chat (IRC) server [12], point of contact database need to be setup at CSIRTs. FIRe is developed with following 5 main objectives :

a. to explore the options for improvingcommunity-to-CSIRT communication & coordination in cyber security incident resolution.

b. Real Time coordination in incidents as required.

Figure 3.FIRe V 1.0 Screenshot.

Extensions and Functionalities of FIRe

Secure Email- Pretty Good Privacy (PGP)

c. Provide platform for real-time Analyst-to-Analyst coordination.

d. Enable rapid exchange of ideas & technical details.

e. Enhance trust & willingness to share information.

Incident contains confidential details and various CSIRTs provide Pretty Good Privacy (PGP)[13] public key for secure email communication (refer to section 3). Mailvelope 0.9.0 [14] is used with FIRe V 1.0 to provide key generation, key management and integration facility with email service providers for secure email communication with CSIRTs and other entities as required during incident reporting & resolution phases.

Figure 4. Secure Email Communication-Mailvelope.

Information Sharing-Traffic Light Protocol (TLP)

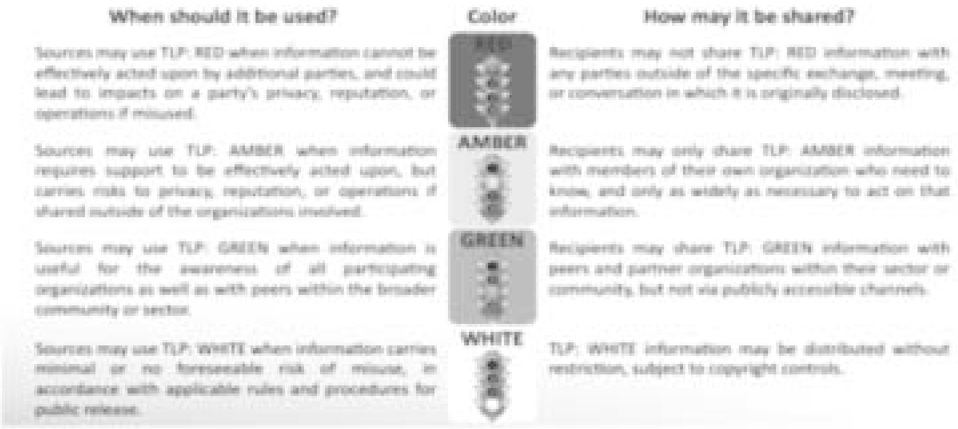
TLP [15] is used by various international CERTs for marking confidential information by incident reporter and ensures controlled disclosure. It make use of four colors (Red, Amber, Green, and White) to classify information according to sensitivity, refer figure 4 (Source: US-CERT). FIRe ensures marking of information as per TLP in incident reporting, IoC sharing and during real time coordination.

Real Time Coordination-Internet Relay Chat (IRC)

Internet Relay Chat(IRC) [12] provides real time group chat facility. Instant Messaging (IM) and IRC are useful in incident resolution for analyst-to-analyst coordination, informal and fast sharing of ideas & technical details. FIRe v 1.0 uses Chatzilla 0.9.90.1 [17] as IRC client. In FIRe V 2.0, it is proposed to include common instant messaging (IM) client that would support IRC, XMPP/Jabber [18] and IM web services.

Incident Reporting Portal

This feature enable web-based secure incident reporting as per incident reporting form of CERT-In [19] to national/sectoral CSIRTs. This system improves collection of required incident related information. Incident reporting portal reduces the time required for resolving the incident and also improve efficiency of CSIRT.



When should it be used?	Color	How may it be shared?
Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	RED	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.
Sources may use TLP: AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	AMBER	Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.
Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	GREEN	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	WHITE	TLP: WHITE information may be distributed without restriction, subject to copyright controls.

Figure 5. Information Sharing Traffic Light Protocol (Source: US-CERT[16]).

Sharing Indicators of Compromise (IoC)

IoC are artifacts that indicate a computer security incident. IoC typically includes IP addresses, MD5 hashes of files, other attributes of malicious files, URL of botnets. IoC provides fast threat information exchange for early intrusion detection and threat data correlation at CSIRT. Organizations unwilling to share complete incident information should be encouraged to share IoC. FIReprovide portal for sharing the IoC with trusted entities.

Integration of cyber threat management systems like Collective Intelligence Framework (CIF) client in FIRe

FIRe will provide client interface for accessing threat management system-Collective Intelligence Framework (CIF). "*CIF allows you to combine known malicious threat information from many sources and use that information for identification (incident response), detection (IDS) and mitigation (null route). The most common types of threat intelligence warehoused in CIF are IP addresses, domains and urls that are observed to*

Figure 6. Internet Relay Chat(IRC) client- Chatzilla.

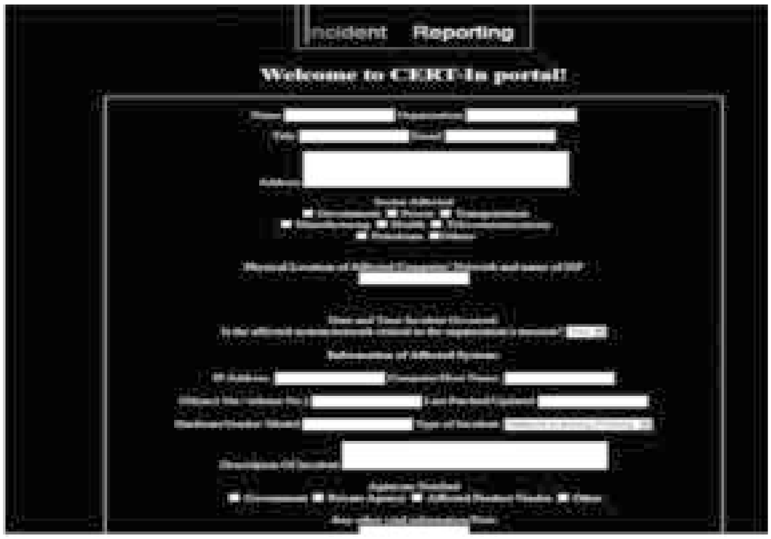


Figure 7. Incident Reporting Portal.

be related to malicious activity"(source: Google-code-CIF description)[20]. This functionality will allow access to threat information shared by community and collected by cif from various sources on internet, as configured by CSIRT like malwaredomainlist [21] and spamhaus [22].

Security advisory, vulnerability and alert notes by feed reader to the subscribers

During study of means of communication implemented by CSIRTs (refer section 3), it is observed that various CSIRTs implemented feeds for sharing vulnerability report, security alert and advisory. Sage 1.5.2 [23] is implemented with FIRe for RSS and Atom feed aggregation.

Dashboard for sharing internet weather based on NetFlow sensors data

FIRe display Internet weather – "current observed threat level" based on the data collected by the network sensors and network data analysis systems implemented by CSIRT at national level or by sectoral CSIRT for specific sector.

Stakeholders and service provider's point of contacts (PoC) Database.

Coordination with various domestic and international entities is required to resolve the incident. Organizations usually maintain details of PoC in their security plan, however the database is limited to few entities & service providers and may not include PoC

Table 1. FIRe functionality Implementation [Yes(Y), No(N), Not Applicable (NA)].

Functionality/Version	FIRe V1.0	FIRe V2.0
Secure Email	Y	Y
Information Classification -TLP	Y	Y
Real Time Coordination-IRC client	Y	NA
Real Time Coordination-Common IM Client	N	Y
Incident Reporting Portal	Y	Y
Sharing Indicators of Compromise	Y	Y
Cyber Threat Management Systems-Integration	N	Y
Feeds-Security advisories, alerts from CSIRTs to users	N	Y
Point of Contact Database	N	Y

of vectors involved in particular incident. FIRe will provide access to the centralized database of PoCs maintained by CSIT.

FIRe version 2.0 is planned for development after evaluation of FIRe 1.0 in upcoming cyber security exercise, discussed in next section. Table below provides snapshot of features implemented/proposed to implement in respective versions of tool.

Fire in Cyber Security Exercise

Indian Computer Emergency Response Team (CERT-In) is conducting national cyber security exercises (CSE) on periodic basis targeting various sectors of the Indian economy. The purpose of exercises is to provide opportunity to the participating organizations to test their preparedness in combating cyber attacks by means of preparation, detection, reporting, coordination & communication, mitigation and response actions. Cyber security exercises also provide opportunity to improve coordination & communication activities among national CERT, sectoral CERTs, stakeholders and service providers. It is proposed to include FIRe in forthcoming exercise as a one window solution for incident reporting, Instant Messaging, secure email communication, sharing artifacts & logs and Point of contacts database of CERTs/stakeholders/agencies/service providers. Cyber security exercise will provide platform for FIRe operational testing. Learning & feedback of exercise observer team and participating organizations will be used to improve the FIRe before releasing it for community use.

Conclusion

Author believe that FIRe will have positive impact in incident reporting and resolution activities. FIRe will improve coordination and communication among organizations, sectoral CSIRTs, service providers and national CSIRT. Browser plugin based implementation made it platform independent and easy to setup. It will improve the operational efficiency of CSIRT by flourishing culture of standardize coordination & communication in incident reporting and resolution. FIRe can be further enhanced with functionality to collect threat information and incident information from international partners and vendors. National/ sectoral CSIRT may add the functionality for pushing vulnerability reports, critical threat alerts, malware alerts, network flow analysis trends to the sector or organizations using the FIRe. FIRe evaluation in upcoming cyber security exercise will definitely lead us further.

References

1. European Union Agency for Network and Information Security (ENISA), http://www.enisa.europa.eu/.
2. European Union Agency for Network and Information Security (ENISA): Annual Incident Reports 2012. Analysis of Article 13a incident reports.
3. ENISA: Article 13a Expert Group portal. https://resilience.enisa.europa.eu/article-13.
4. Moira J. West-Brown, Don Stikvoort, and Kalus-Peter Kossakowski: *Handbook for Computer Security Incident Response Teams(CSIRTs).*CMU/SEI-2003-HB-002.
5. CERT-In Monthly Report, http://www.cert-in.org.in/.
6. KimoonJeong, Junhyung Park, Minsoo Kim, BongNam Noh: A Security Coordination Model for an Inter-Organizational Information Incidents Response Supporting Forensic Process. *IEEE Fourth International Conference on Networked Computing and Advanced Information Management (2008).*
7. Hennin, S., Control System Cyber Incident Reporting Protocol. *IEEE, Technologies for Homeland Security (2008).*
8. Indicators of Compromise (IoC), https://www.mandiant.com/blog/tag/openioc/.
9. James R. Antonides, Donald N. Benjamin, Daniel P. Feldpausch, and Jeffrey S. Salem, USCC :Streamlining the US Army Network Incident Reporting System. *Proceedings of the 2008 IEEE Systems and Information Engineering Design Symposium.*

10. CERT/CC:http://www.cert.org/incident-management/national-csirts/national-csirts.cfm.

11. Mozilla Firefox. http://www.mozilla.org/.

12. Internet Relay Chat (IRC). http://tools.ietf.org/html/rfc1459.html.

13. PGP: http://www.ietf.org/rfc/rfc2440.txt.

14. Mailvelope: https://www.mailvelope.com/.

15. Information Sharing Traffic Layer Protocol (ISTLP): https://www.enisa.europa.eu/activities/cert/support/incident-management/browsable/incident-handling-process/information-disclosure.

16. United States Computer Emergency Readiness Team (US-CERT). https://www.us-cert.gov/.

17. ChatZilla. https://addons.mozilla.org/en-US/firefox/addon/chatzilla/.

18. XMPP/Jabber. http://www.ietf.org/rfc/rfc3920.txt.

19. Indian Computer Emergency Response Team (CERT-In). http://www.cert-in.org.in.

20. Collective Intelligence Framework. https://code.google.com/p/collective-intelligence-framework/.

21. malwaredomainlist. http://www.malwaredomainlist.com/.

22. Spamhaus. http://www.spamhaus.org/.

23. Sage 1.5.2. https://addons.mozilla.org/en-US/firefox/addon/sage/.