GN3-JRA2/T4 update on X-ARF

Tilmann Haak, Jan Kohlrausch, Torsten Voß (DFN)
Simona Venuti (GARR)

TF-CSIRT, Rome, 30 January 2012

Content

- JRA2/T4 Overview and Subtasks
- Questions / Problems / Proposal / Share experiences with TF-CSIRT Community

JRA2/T4 Overview

- Research in finding new threats
- Research on finding reliable list of BotNet Server or "bad hosts"
- Research methods to find problems and to notify them inside a multi-domain environment
- Research on how to harmonize the format of communications inside multi-domain enviromnent
- Trying to make things as automatic as possible

Subtask List

- **Sub1- HoneyPot:** studying and implementing a test environment for HoneyPot systems
- **Sub2- Anomaly Detection:** algorithms to find anomalies in NetFlow traffic, BotNet traffic detection, anomaly detection in DNS traffic
- **Sub3 - The Tool(s):** develop new plugins filled by Sub1 and Sub2, and plugins to transmit automatically the information in a multi-domain environment: **NfQuery**
- **Automatization, Collaboration:** common format to exchange information
- **Network Devices:** security aspects embedded in network devices

Introducing “our” X-ARF problem

- We found that X-ARF is the best suitable format to exchange information between entities involved in a security incident
- We wrote internal deliverables about privacy issues against X-ARF format, and how to use honeypots to support incident handling
- X-ARF works well for single reports. But we came accross the point, that X-ARF via email is inefficient for bulk data and we are currently investigating solutions to that problem
- We then studied an extended specification for the X-ARF format to aggregate multiple incidents involving the same IP
- We encountered many difficulties and problems in trying to make everything work

Introducing “our” X-ARF problem

- In the next slides the details of these problems:

  “The Aggregation Problem”

- We are here to ask to TF-CSIRT Community if they have ever deal with this issues, if YOU want to share experiences in this X-ARF issue

- (and if you already have a solution for them ☺)

Conclusion

Thank-You

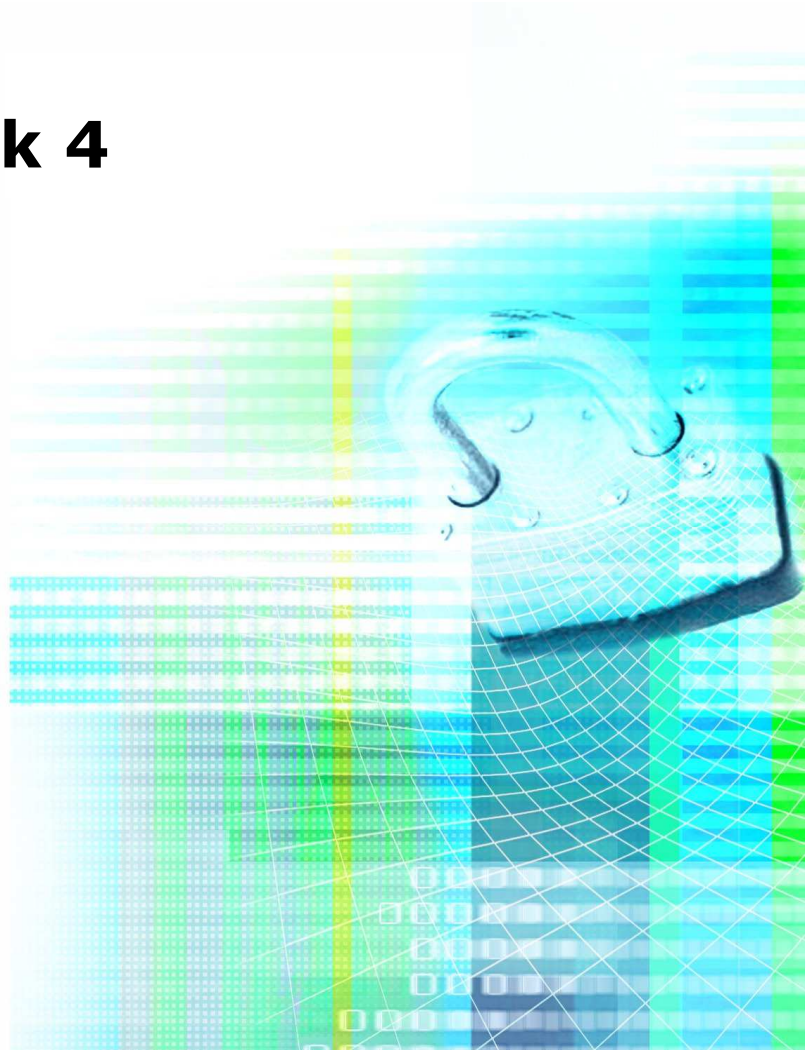
simona.venuti@garr.it

Update on the X-ARF Format

Rome 2012 / Géant 3 Task 4

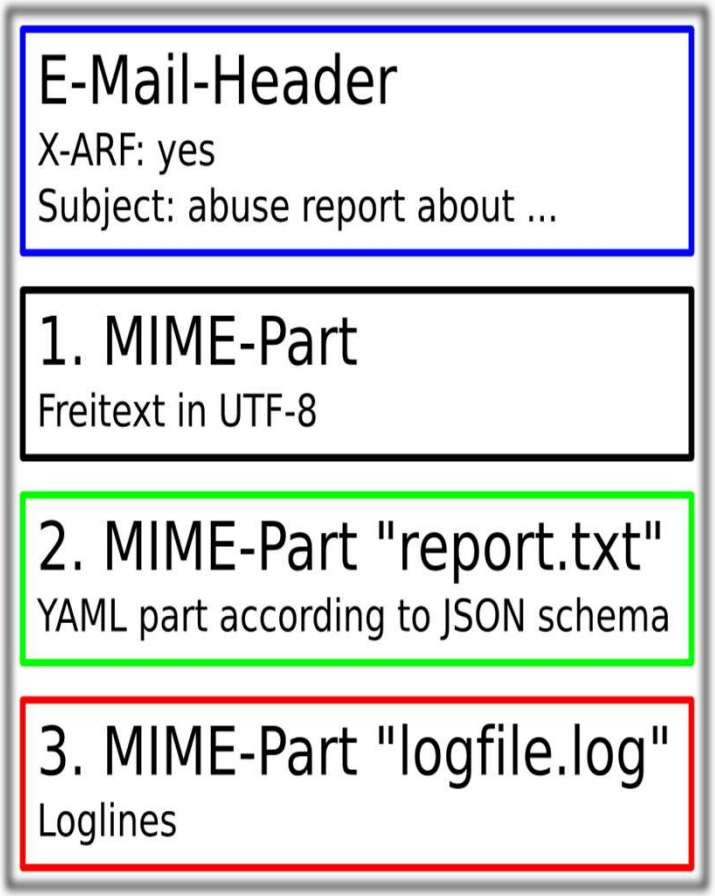
Tilmann Haak
Jan Kohlrausch
Torsten Voß

DFN-CERT Services GmbH



Summary of X-ARF

- What is X-ARF:
  - Lightweight structured data exchange format (Yaml/Json)
  - Independent of data source (e.g. supports IDS, honeypot data, and service log-data)
  - Based on MIME for email transport
- What X-ARF is not:
  - Storage format (e.g. for relational databases)

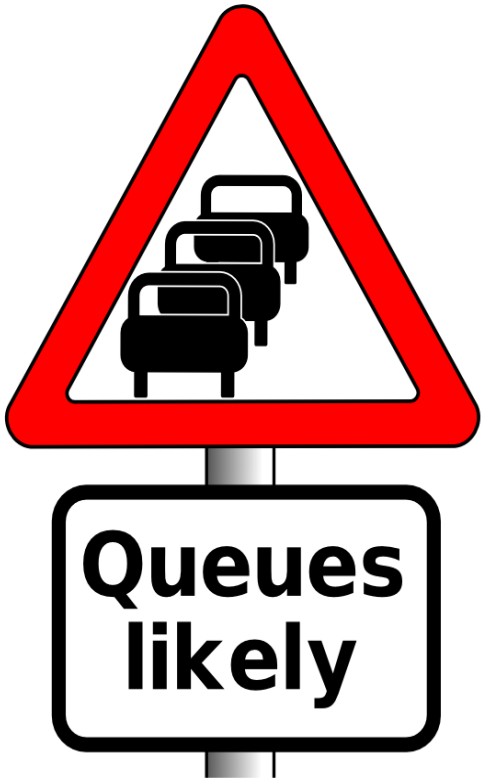


Advantages of X-ARF

- X-ARF is great, because:
  - Structured format allows automated processing
  - Easy to process
  - Can be directly sent to affected sites (Human readable part):
    - No a-priori knowledge about format required
    - Email transport medium is broadly accepted

Disadvantages of X-ARF

- But:
  - Email is disadvantageous for bull data (netflow, honeypot)
  - S/MIME is not supported in curre X-ARF specification
  - Current X-ARF specification suffe from minor ambiguities



Ongoing Work on X-ARF

- Proposed enhancements to clarify the ambiguities of the specification
- Ongoing work to integrate S/MIME into the specification
  - Digital signature
  - Encryption
- Solution for bulk data transfers

Bulk Data Transfer

- Aggregation of multiple reports within a single X-ARF report
- Two different formats have been proposed by DFN-CERT
- But:
  - Textual format is inefficient
  - Would require new programs in order to handle reports
  - Difficult to get standardised

Bulk Data Transfer II

- Detaching X-ARF from the email transport medium:
  - Alternative HTTP-based transport of X-ARF messages
  - No need to change X-ARF Json schema
  - E.g. could use Representational State Transfer (REST)

Questions?

Tilmann Haak <haak@dfn-cert.de>

Jan Kohlrausch <kohlrausch@dfn-cert.de>

Torsten Voß <voss@dfn-cert.de>

https://www.dfn-cert.de/