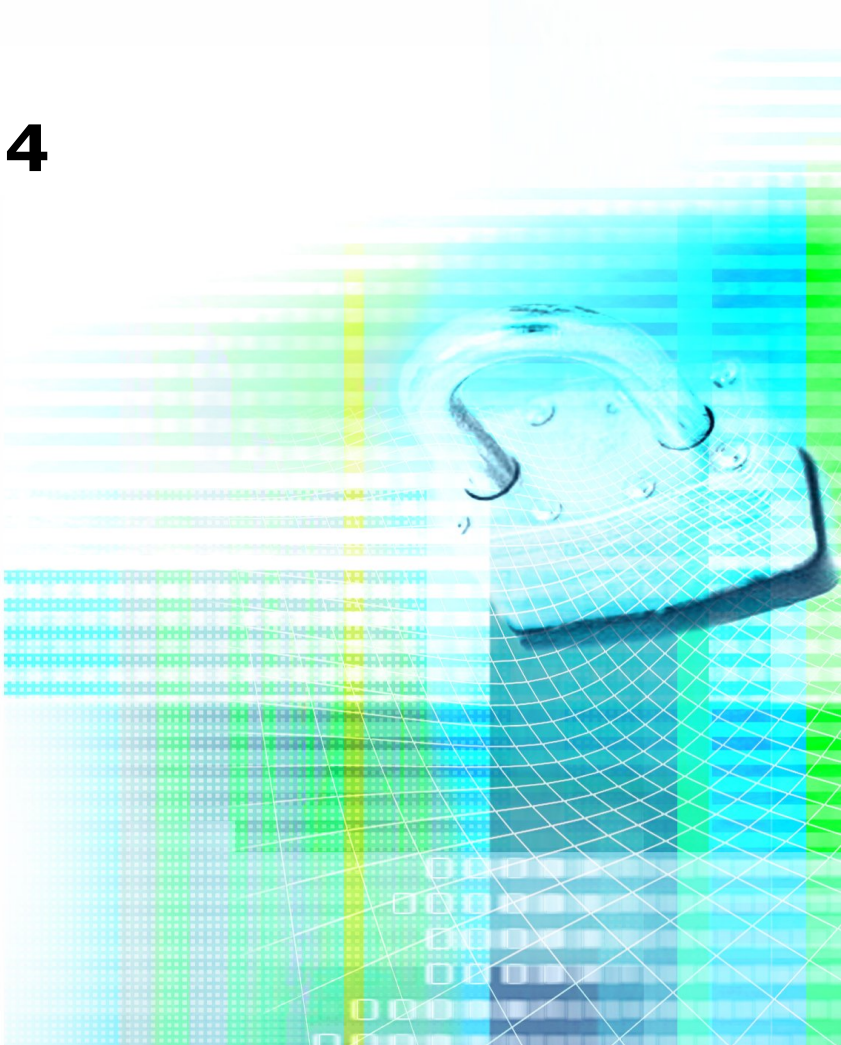
# Update on the X-ARF Format

## Rome 2012 / Géant 3 Task 4

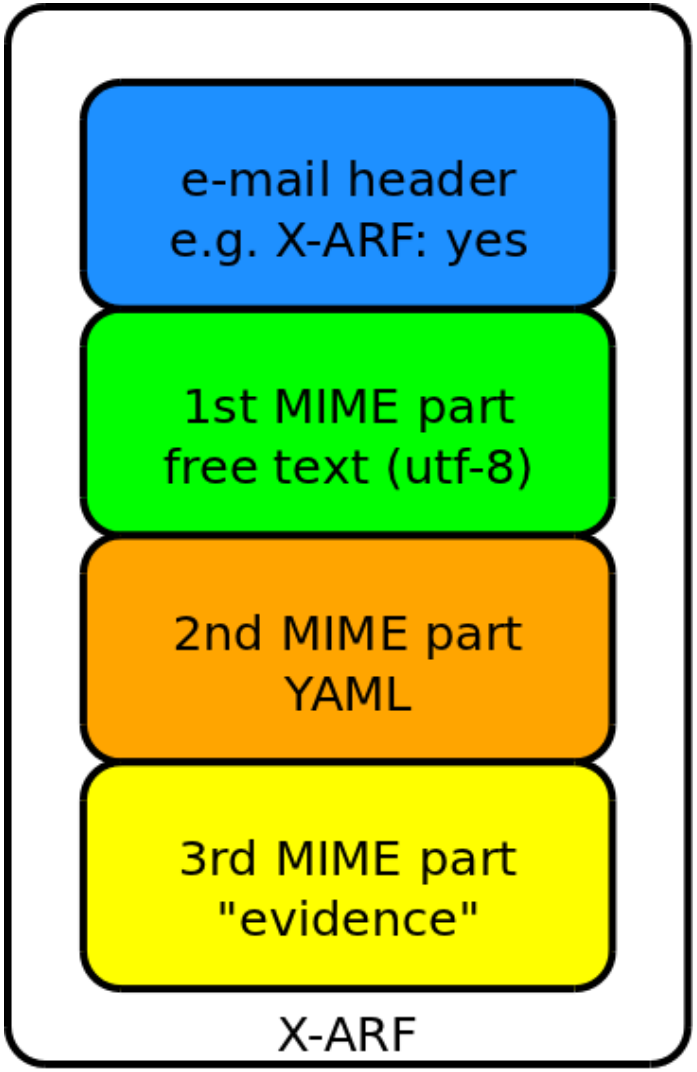
Tilmann Haak
Jan Kohlrausch
Torsten Voß

DFN-CERT Services GmbH



# X-ARF overview

- 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, ...)
  - Uses e-mail for transport
- What X-ARF is not:
  - Storage format (e.g. for relational databases)
  - Protocol



# Advantages of X-ARF

- X-ARF is great, because:
  - Structured format allows automated processing
  - Validation using JSON schemata
  - 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
  - Human- and machine-readable

# Disadvantages of X-ARF

- E-mail is disadvantageous for bulk data (netflow, honeypot, ...)
- S/MIME and PGP/MIME is not supported in current X-ARF specification
- Current X-ARF specification suffers from ambiguities
- Not yet a stable standard

# Ongoing Work on X-ARF

- Proposed enhancements to clarify the ambiguities of the specification
- Ongoing work to integrate S/MIME and PGP/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 bee proposed by DFN-CERT
- However:
  - e-mail format is inefficient
  - Home-grown DDoS?
  - Would require new software in order to handle reports
  - Difficult to get standardised
  - No simple solution

# Bulk Data Transfer II

- Use a bulk schema that contains a list of affected systems.
  - Would be within current X-ARF standard, but it does not fit well
- Multiple YAML parts as a list, referencing multiple named attachments
  - Violates current standard
  - Quite complicated
- Some people say it is unnecessary.
- However for bulk data the human-readable part may be dropped.

# Bulk Data Transfer III

- Detach X-ARF from the e-mail transport medium!
- No need to change X-ARF JSON schema
- HTTP-based transport of X-ARF messages?
- Representational State Transfer (REST)
- FTP? SCP? SFTP? XMPP?
- In general the format is independent of the transport protocol.

# Questions?
# Comments?
# Ideas?

**Tilmann Haak <haak@dfn-cert.de>**

**Jan Kohlrausch <kohlrausch@dfn-cert.de>**

**Torsten Voß <voss@dfn-cert.de>**

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