

## GN3-JRA2/T4 update on X-ARF

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

TF-CSIRT, Rome, 30 January 2012

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

- 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 environment
- Trying to make things as automatic as possible

- **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

- 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 😊)

## Thank-You

[simona.venuti@garr.it](mailto:simona.venuti@garr.it)