

RESTENA Foundation  
TF-MNM 23 sept 2010



# Report on Improving CSIRT collaboration

Stefan Winter - <[stefan.winter@restena.lu](mailto:stefan.winter@restena.lu)>

# Problem Statement

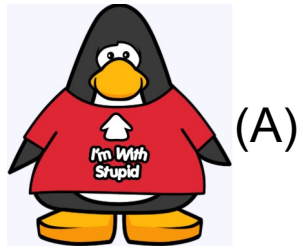


- eduroam Service Description contains only very simple statement regarding security incidents :
  - “Whenever necessary and appropriate, incidents should be handled by the respective CERT(s).”
  - When is it necessary, when appropriate ?
- Plus, there can be as many as three CSIRTs “interested”

# Attack scenario (home server)



attacker's home domain



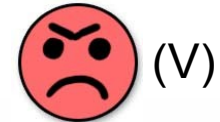
Ronald Duck  
ronald@dismay.com

hotspot



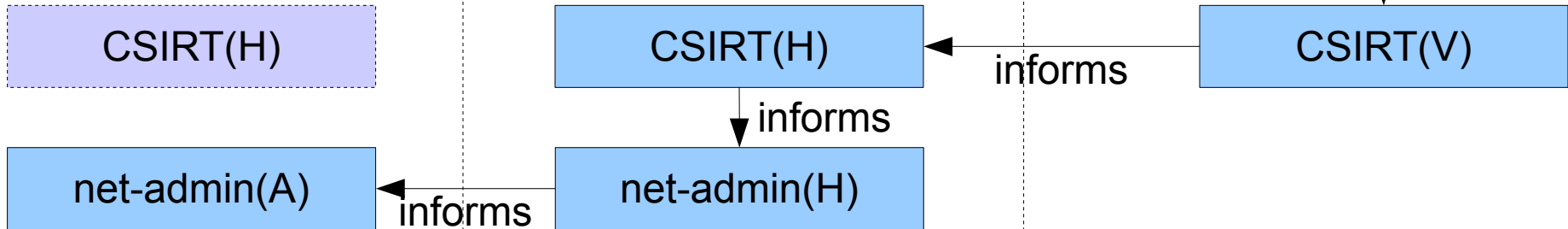
don.stikvoort@dismay.com

victim



attacked from IP  
198.51.100.23

↓ informs



- net-admin(A) checks authentication logs of the authentication in question
- finds out that attacker id is [ronald@dismay.com](mailto:ronald@dismay.com)
- can take appropriate measures of punishment for **Ronald Duck**

# Findings



- Presentation held on 17 sep 2010 (TF-CISRT Seminar)
  - Observation: CSIRTs don't ever hear anything regarding eduroam incidents
    - No incidents?
    - Or just “out of the loop”?
  - CSIRTs would like to be informed cc-style
    - net-admin(H) to inform CSIRT(H)
    - net-admin(A) to inform CSIRT(A)
  - But communication between hotspot and IdP is to follow eduroam procedures (i.e. no CSIRT escalation)

# Consequences



- For every security incident,
  - eduroam SPs MUST inform their CSIRT that hotspot was abused by someone from realm X
  - Eduroam IdPs MUST inform their CSIRT that one of their users has been identified of doing something nasty
- These would be FYI only; with no follow-up expected
- Template forms (FITB) to be prepared