draft-ietf-suit-information-model-04

Brendan Moran
Hannes Tschofenig
Status

• Working Group Last Call started on August 12\textsuperscript{th} by Russ
  
  https://mailarchive.ietf.org/arch/msg/suit/GmzvPrvaxVKN3nyNZKfSwSwBhw

• August is vacation time….  

• Dave Thaler provided extensive review, see
  
  https://mailarchive.ietf.org/arch/msg/suit/9awZNOvRd8MduaX3_6Cu
  vHoxm80

• His review lead to -04.
Justifying E2E security model

• E2E Security was required in the architecture, but not justified.
• Added Threats
• Added Security Requirements
E2E Security Model: Threats

• MITM: Intercept of data between update service and device
• Key Exposure: Extraction of signing keys from signing service
• Manifest Modification: Malware, TLS-unwrapping, phishing, XSS attacks between author and signing service
E2E Security: Requirements

• Reporting: Secure channel for status reports from devices
• Key Protection: Proper storage of signing keys
• Manifest Check: Service-based validation of manifest prior to distribution
• Manifest Trusted: Trusted environment for constructing manifests
More Reviews

• Still some reviews coming in

• Several proposed changes in github:
  • Change MANDATORY to REQUIRED
  • Add example of UUIDs for white-labelling
  • Explicitly disallow channel security for update authentication
    • Similar lightweight authentication can be done with COSE_MAC
    • MAC keys are subject to REQ.SEC.KEY.PROTECTION
  • Define maximum size of integrated payload
Next Steps

• Asked further reviewers for confirmation that the document is complete.
• Document complete from the point of view of the authors.