IRTF
Decentralized Internet Infrastructure Proposed Research Group
DISS Workshop Preview

Interim Meeting at NDSS-2018

Carsten Bormann, Dirk Kutscher, Michael McCool, Pekka Nikander, George Polyzos, Thomas Schmidt, Matthias Wählisch

2018-02-17, San Diego, CA, USA

NDSS Workshop on **Decentralized IoT Security and Standards (DISS)**

- https://www.ndss-symposium.org/ndss2018/cfp-ndss2018-diss/
- Sunday, February 17, 2018

- IoT success depends on solving underlying security and privacy challenges
- Due to scale of deployment and limited resources, some systems will be extremely challenging to secure
- One key aspect: decentralization
  - Many if not most of IoT scenarios include intermittent connectivity
  - Decentralized security may help to overcome privacy concerns and scalability bottlenecks
  - Important for large-scale deployments, such as smart cities or Industry 4.0

DISS Motivation

- **Decentralized approach to IoT security: many opportunities & challenges**
    - Operating with constrained device and network capabilities
    - State synchronization
    - Trust management
- **Many IoT standards are now under development**
    - IETF CoAP, OCF, and LWM2M)
    - W3C Web of Things
    - Many of these implicitly or explicitly support metadata and have interoperability as goals
    - Raising new security and privacy issues that need to be discussed and addressed
    - Systems composed of multiple standards also raise challenges
        - for example, how to maintain security across bridges and how to evaluate trust across standards boundaries

DISS Scope

- **Enabling secure interoperability across IoT ecosystems**
    - Applying blockchains and Distributed Ledger Technology to IoT infrastructure
    - Security and availability in multi-tiered IoT edge networks (“fog computing”)
    - Peer-to-Peer security and privacy (P2P) in IoT
    - Decentralized trust and rights management, including access control
    - Decentralized authentication and access management at the IoT edge
- **Security and privacy in ongoing IoT standardisation work**
    - Security and privacy in W3C Web of Things, OCF, IETF CoRE and ACE, etc.
    - Semantic modeling and descriptive approaches for security
    - Convergence/divergence between web, fog, cloud, and IoT security standards
    - Decentralized IoT security architectures for 5G Networks
    - Privacy, identity, and metadata management
    - Integrating “multi-standard” systems with different levels of security and trust
- **Other topics related to decentralized security and standardization in IoT**
    - Security and privacy trade-offs related to IoT scalability and decentralization
    - Secure Service provisioning and migration in IoT
    - Sensor and Actuator Key Management and other Security Protocols
    - Smart Contracts for IoT, including formal verification of smart contracts
    - Application of concepts from outside of the IoT to decentralized IoT security
    - Usable security for decentralized IoT

DISS Program Overview

- **Smart Contracts**
  - Ledger federation
  - Secure payments for edge computing
- **Usable Security for Decentralized IoT**
  - Network anomaly detection
  - Authentication, key exchange
  - Blockchain cosigning reliability
  - Authorization in IoT
- **Standardizing IoT Security**
  - Policy enforcement
  - Web of things security
  - Security Economics
- **Practical Aspects and Attestation**
  - Lightweight Blockchain clients
  - IoT runtime and user-centered-attestation

DISS Program (1)

Smart Contracts	
Secure Open Federation for Internet Everywhere	Arto Karila, Yki Kortesniemi, Dmitrij Lagutin, Pekka Nikander, Nikos Fotiou, George Polyzos, Vasilios Siris and Theodore Zahariadis
SPOC: Secure Payments for Outsourced Computations	Michał Król and Ioannis Psaras
Usable Security for Decentralized IoT	
CIoTA: Collaborative Anomaly Detection via Blockchain	Tomer Golomb, Yisroel Mirsky and Yuval Elovici
A Lightweight Authentication and Key Exchange Protocol for IoT	Abdulrahman Bin-Rabiah, K. K. Ramakrishnan, Elizabeth Liri and Koushik Kar
Reliable Collective Cosigning to Scale Blockchain with Strong Consistency	Bithin Alangot, Maneesha Suresh, Arvind S Raj, Rahul Krishnan Pathinarupothi and Krishnashree Achuthan
Avoiding Gaps in Authorization Solutions for the Internet of Things	Stefanie Gerdes, Olaf Bergmann and Carsten Bormann

DISS Program (2)

Standardizing IoT Security	
Standardizing IoT Network Security Policy Enforcement	David Barrera, Ian Molloy and Heqing Huang
Distributed Security Risks and Opportunities in the W3C Web of Things	Michael McCool and Elena Reshetova
Exploring Security Economics in IoT Standardization Efforts	Philipp Morgner and Zinaida Benenson
Practical Aspects and Attestation	
Unifying Lightweight Blockchain Client Implementations	Gruber Damian, Wenting Li and Ghassan Karame
Practical Runtime Attestation for Tiny IoT Devices	Stefan Hristozov, Johann Heyszl, Steffen Wagner and Georg Sigl
User-Centred Attestation for Layered and Decentralised Systems	Hagen Lauer, Ahmad Salehi, Carsten Rudolph and Surya Nepal