PRivacy preserving pOst-quantuM systEms from
advanced crypTograpHic mEchanisms Using latticeS

Aggregating Cyber Threat Intelligence while preserving confidentiality

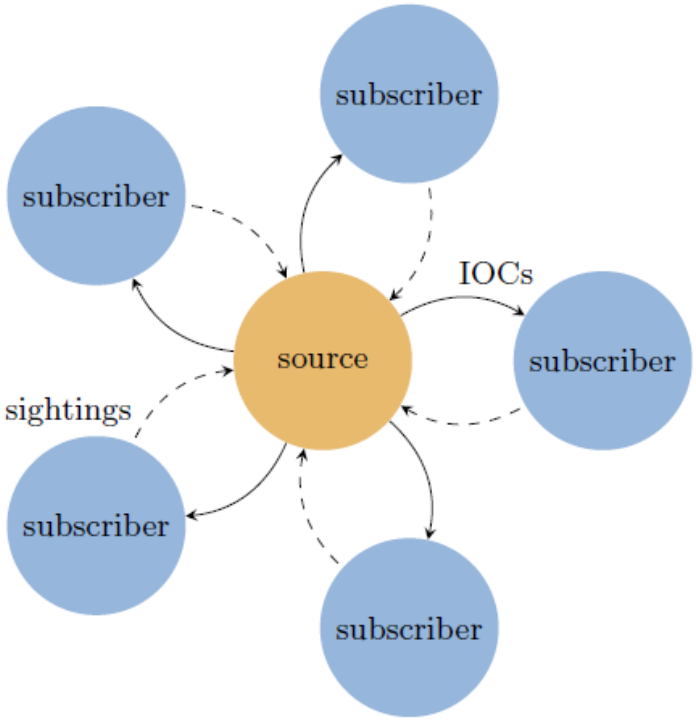
Dr. Gabriele Spini, TNO

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780701.

Use case: CTI

- Organisations have cyber threats in their IT infrastructure
- Measures to reduce these threats are costly
- Exchanging sensitive threat information between organisations increases insight and reduces costs; but organisations are hesitant to share the information for fear of reputation damage
- Ability to report hits in an anonymous way increases participation and thus situational awareness.

CTI community



IOCs and Sightings

- IOC:


```
{
    "type": "indicator",
    "id": "indicator--71312c48-925d-44b7-b10e-c11086995358",
    "created": "2017-02-06T09:13:07.243000Z",
    "modified": "2017-02-06T09:13:07.243000Z",
    "name": "CryptoLocker Hash",
    "description": "This file is a part of CryptoLocker",
    "pattern": "[file:hashes.'SHA-256' =
'46afeb295883a5efd6639d4197eb18bcba3bff49125b810ca4b9509b9ce4dfbf']",
    "labels": ["malicious-activity"],
    "valid_from": "2017-01-01T09:00:00.000000Z"
}
```


- Sighting:


```
{
    "type": "sighting",
    "id": "sighting--4eebf1e1-5351-49ed-9b7b-28f0da806d82",
    "created": "2017-02-07T20:08:31.154Z",
    "modified": "2017-02-07T20:08:31.154Z",
    "sighting_of_ref": "indicator--71312c48-925d-44b7-b10e-c11086995358"
}
```

Obstacles to effective CTI community

Sharing of IoCs occurs regularly,
Sending sightings: much less

- Unclear incentive
- Confidentiality risks: admit having been affected (in some way) by threat

Encryption of CTI information

Could do even more than sightings: add

- Number of hits;
- Incurred (financial) damage.

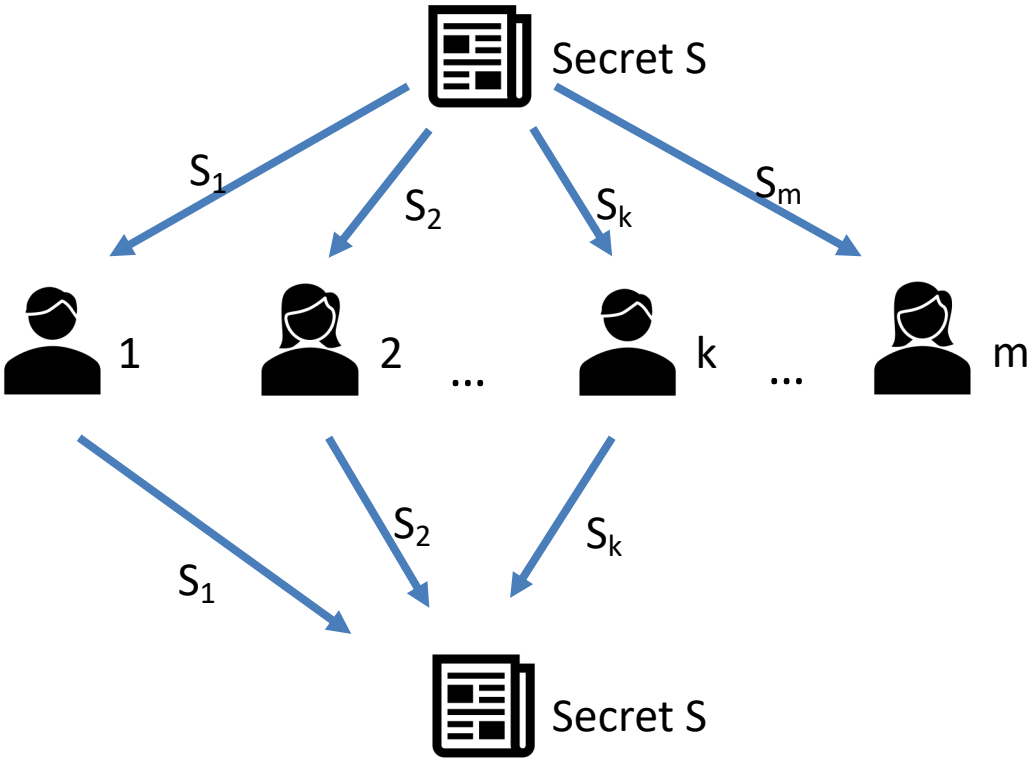
Even more confidential!

Exchanged in encrypted way, aggregated anonymously

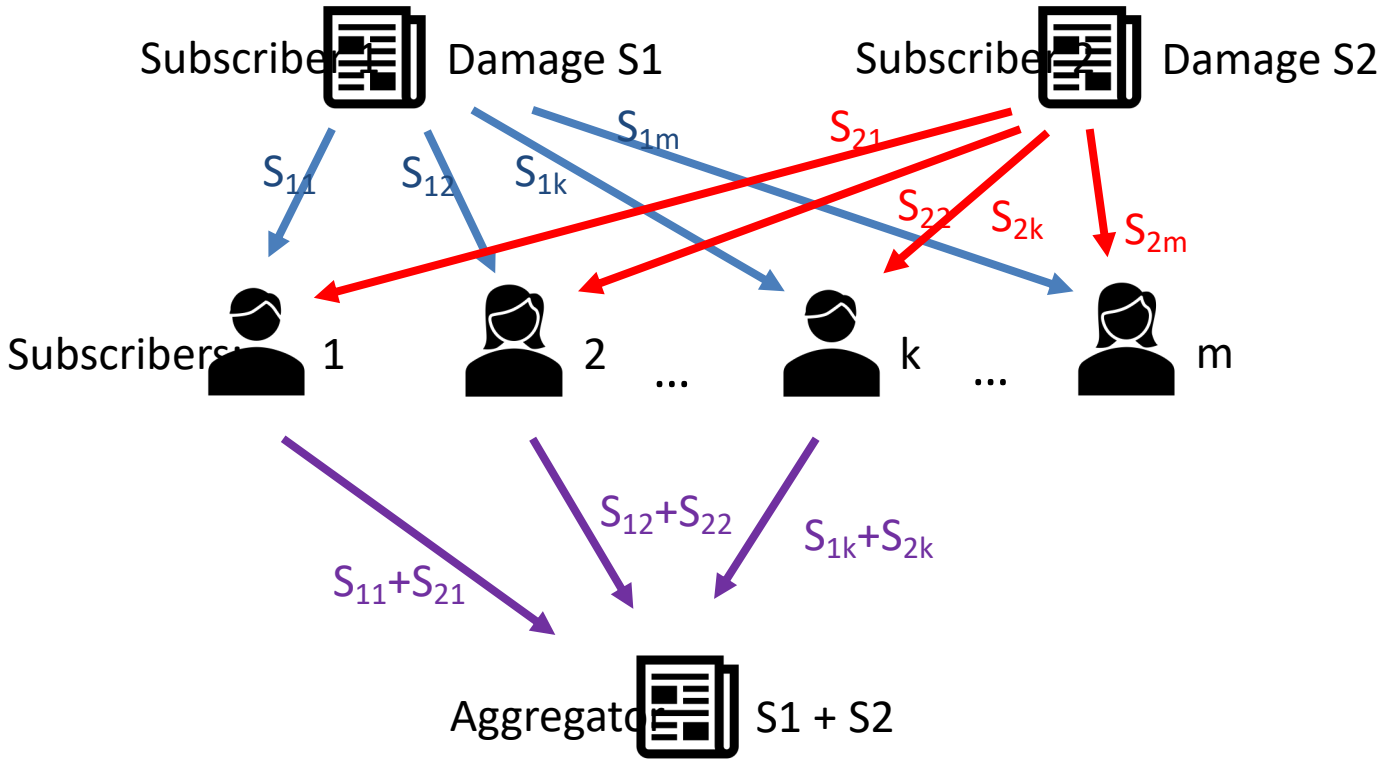
Done by:

1. Shamir secret sharing
2. Encrypting, signing shares
   with lattice-based Post-Quantum Cryptography

Basic Shamir secret sharing



Shamir SS with local addition



Status of Implementation

- The solution is implemented in a Python proof-of-concept
- Interface with MISP (Malware Information Sharing Platform) via custom “object” structure
- In near future (current plan: July 2022):
  - Made available open-source in COSSAS initiative
  - Mirror on MISP github group
  - Blog post describing solution

Demo time!

[Drumrolls]

[Silent prayer to Murphy]