Securing IoT Networks with Onion Routing

15/12/2022

// Julian Schwarzenböck, 11723121
// Alexander Irsigler, 12229935
// Teodor J. Podobnik, 12206639

Agenda

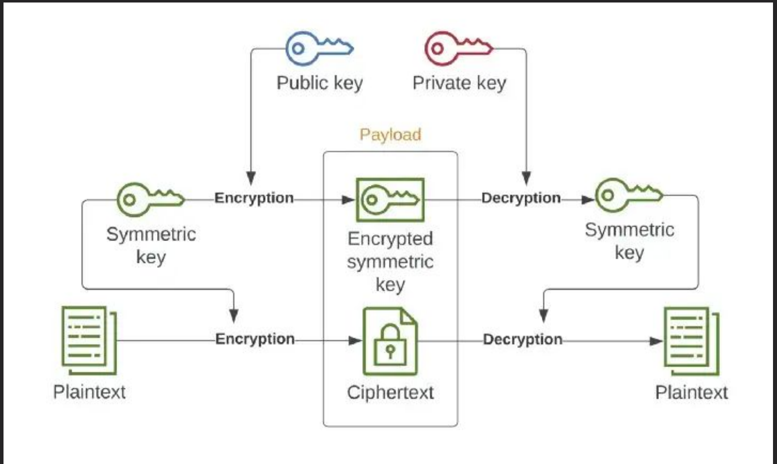
- Problem outline
- Solution breakdown
- Current state
- DEMO TIME!

Problem outline

- Abundance of IoT devices
  - Smart Cities
  - In-Room automation
  - Sports
- User data
  - What user data is stored and tracked?
  - With whom this user data is shared?
  - Why should a user even worry about this?

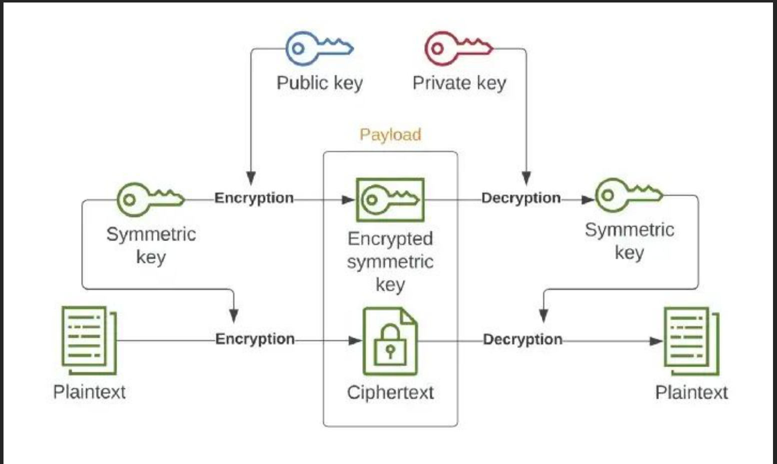
Solution Breakdown

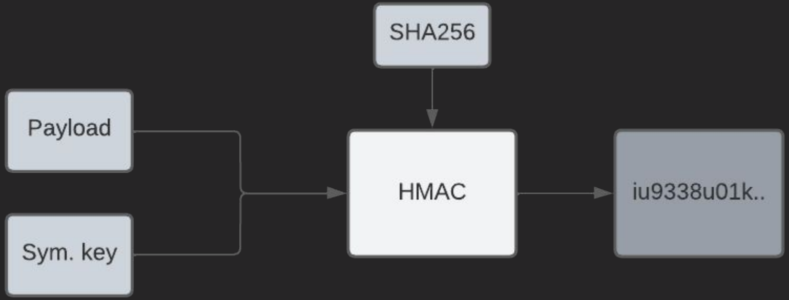
- **Secrecy** - Hybrid encryption
    - Unique sym. key per Chain node
    - Unique PKI per Chain node



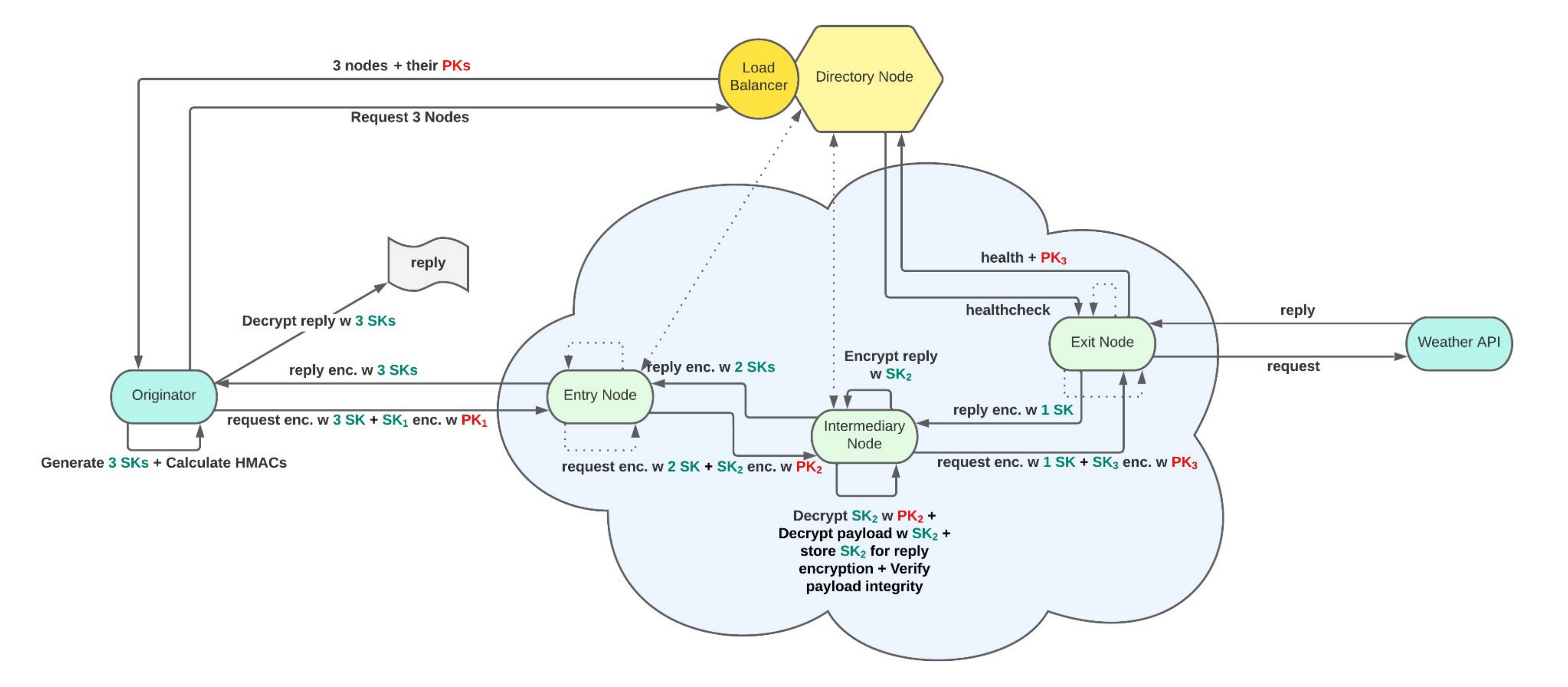
Solution Breakdown

- **Secrecy** - Hybrid encryption
  - Unique sym. key per Chain node
  - Unique PKI per Chain node
- **Integrity** - HMAC (Request only)
- **ANONYMITY** - Onion Routing with Padding

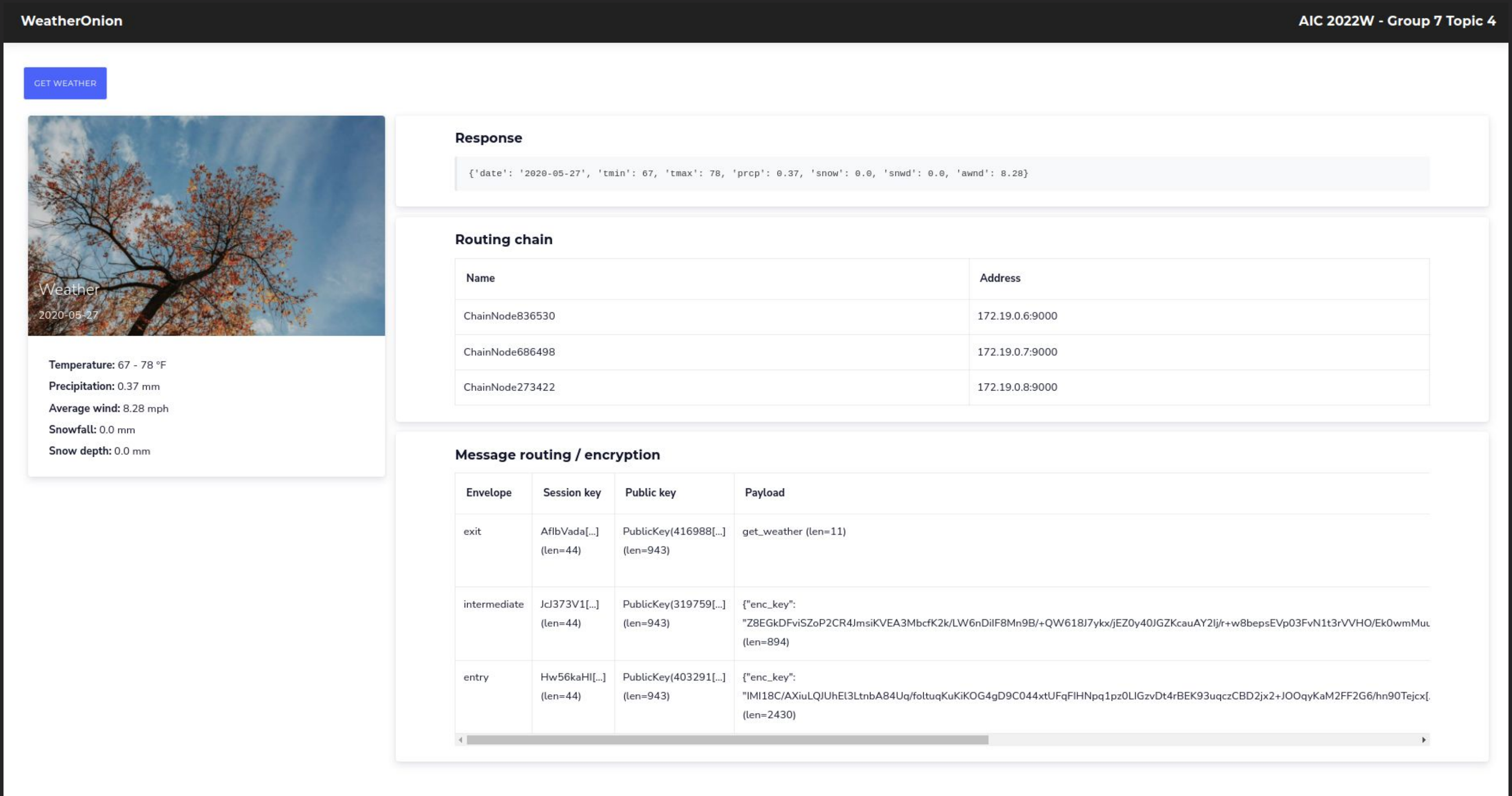




Backend


3 nodes + their PKs
Load Balancer
Directory Node
Request 3 Nodes
reply
Decrypt reply w 3 SKs
health + PK_3
healthcheck
reply
Exit Node
Weather API
request
Originator
reply enc. w 3 SKs
Entry Node
reply enc. w 2 SKs
Encrypt reply w SK_2
reply enc. w 1 SK
Intermediary Node
request enc. w 3 SK + SK_1 enc. w PK_1
request enc. w 2 SK + SK_2 enc. w PK_2
request enc. w 1 SK + SK_3 enc. w PK_3
Generate 3 SKs + Calculate HMACs
Decrypt SK_2 w PK_2 + Decrypt payload w SK_2 + store SK_2 for reply encryption + Verify payload integrity

Frontend



Temperature: 67 - 78 °F
Precipitation: 0.37 mm
Average wind: 8.28 mph
Snowfall: 0.0 mm
Snow depth: 0.0 mm

Response

```
{'date': '2020-05-27', 'tmin': 67, 'tmax': 78, 'prcp': 0.37, 'snow': 0.0, 'snwd': 0.0, 'awnd': 8.28}
```

Routing chain

Name	Address
ChainNode836530	172.19.0.6:9000
ChainNode686498	172.19.0.7:9000
ChainNode273422	172.19.0.8:9000

Message routing / encryption

Envelope	Session key	Public key	Payload
exit	AflbVada[...] (len=44)	PublicKey(416988[...] (len=943)	get_weather (len=11)
intermediate	JcJ373V1[...] (len=44)	PublicKey(319759[...] (len=943)	{"enc_key": "Z8EGkDFviSZoP2CR4JmsiKVEA3MbcfK2k/LW6nDiIF8Mn9B/+QW618J7ykx/jEZ0y40JGZKcauAY2Ij/r+w8bepsEVp03FvN1t3rVVHO/Ek0wmMu (len=894)
entry	Hw56kaHI[...] (len=44)	PublicKey(403291[...] (len=943)	{"enc_key": "IMI18C/AXiuLQJUhEl3LtnbA84Uq/foltuqKuKiKOG4gD9C044xtUFqFIHNpq1pz0LIGzvDt4rBEK93uqczCBD2jx2+JOOqyKaM2FF2G6/hn90Tejcx[(len=2430)

DEMO TIME