Forensic Analysis of Artifacts in the Matrix Protocol and Riot.IM application

By:
Guido Schipper, Rudy Seelt and Nhien-An Le-Khac

From the proceedings of
The Digital Forensic Research Conference
DFRWS EU 2021
March 29 - April 1, 2021

Forensic Analysis of Matrix Protocol and Riot.im Application

Guido Schipper

Nhien-An Le-Khac

Rudy Seelt

DFRWS 2021 VIRTUAL EUROPE

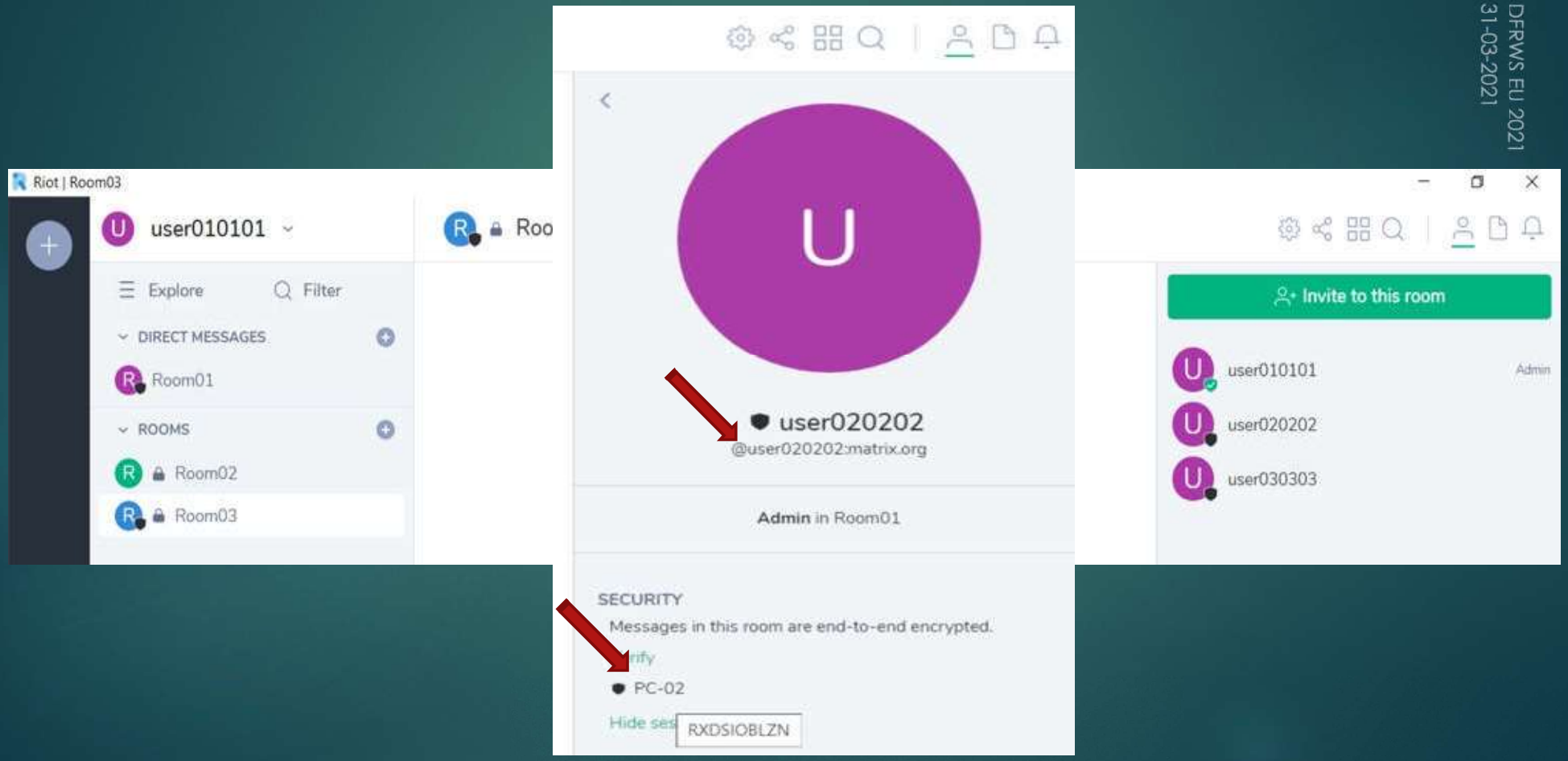
Introduction

- Matrix protocol and Riot.im
- History
- Knowledge gap
- Research goal

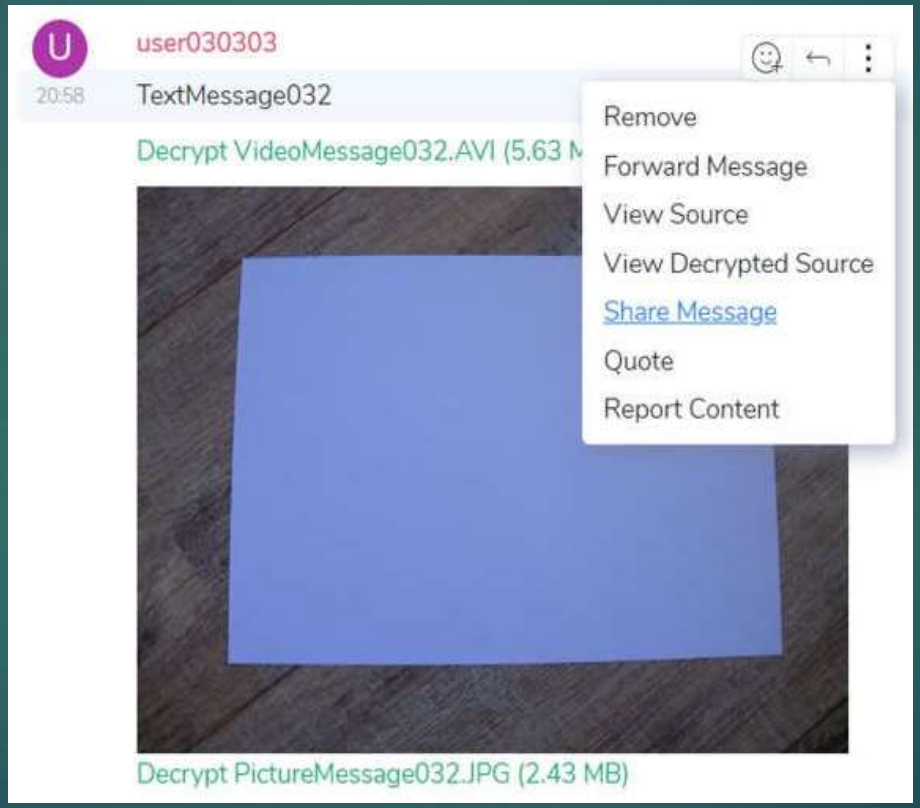
Methodology

- Riot.im application analysis
- Matrix protocol analysis
- Artifact analysis
- Disk analysis

Riot.im application analysis



Riot.im application analysis



Protocol analysis
Events

- Communication between components in the network
- JSON format
- Event categories:
  - State events
  - Message events

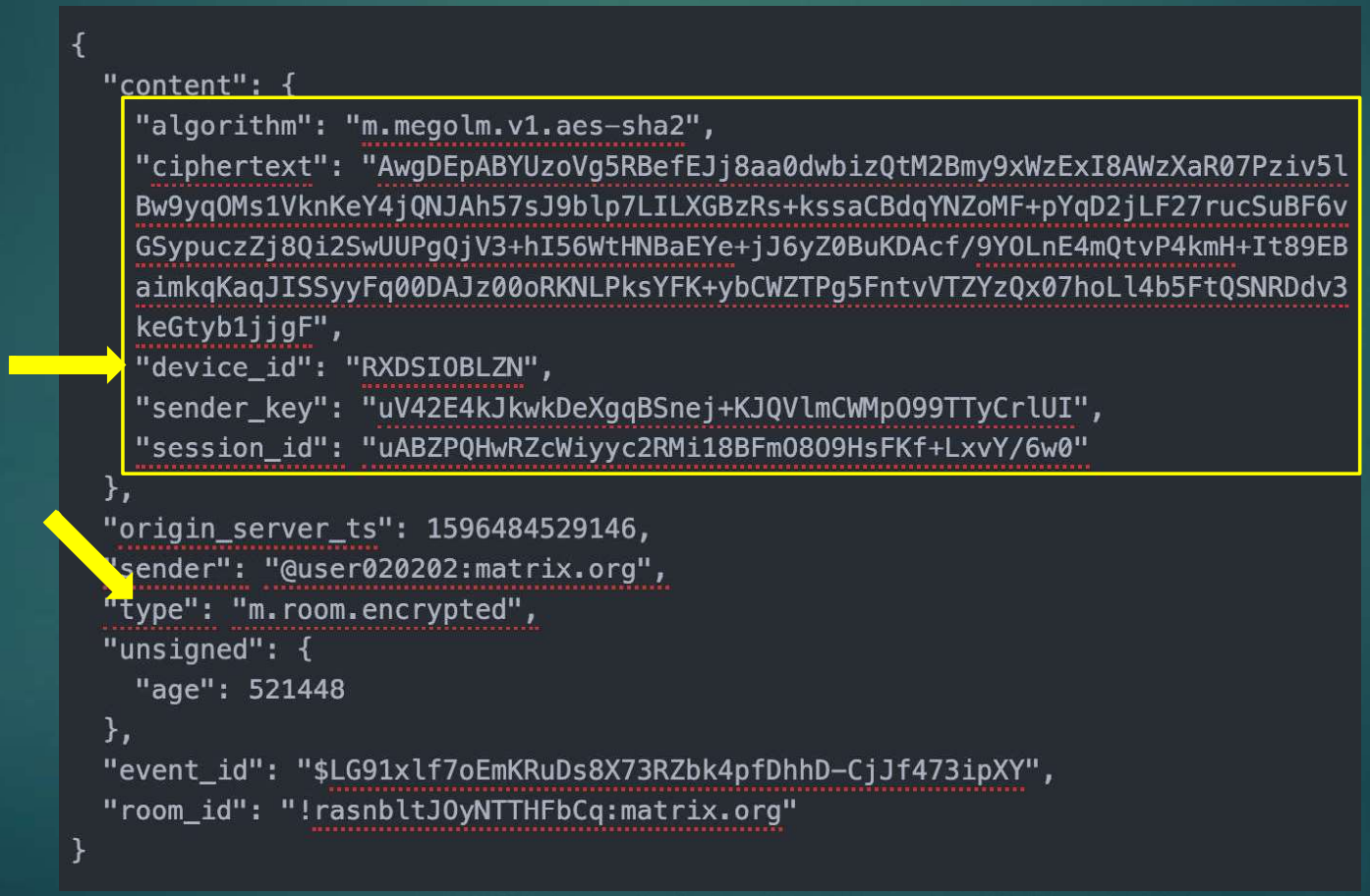
Protocol analysis
Event storage and signing

- Multiple participating servers
- Room graph
- Signing of events

Protocol analysis
Event (example)

```
{
  "content": {
    "body": "test",
    "msgtype": "m.text"
  },
  "origin_server_ts": 1596399135204,
  "sender": "@user010101:matrix.org",
  "type": "m.room.message",
  "unsigned": {
    "age": 121,
    "transaction_id": "m1596398240724.0"
  },
  "event_id": "$1hFZ7QdjE2wN4PR6Z4DlZvUMBbgegDkjlAMf6LvjX5Q",
  "room_id": "!ebYlkYiBNdbfSNCQgl:matrix.org"
}
```

Protocol analysis
Event types (examples)




```
{
  "content": {
    "algorithm": "m.megolm.v1.aes-sha2",
    "ciphertext": "AwgDEpABYUzoVg5RBefEJj8aa0dwbizQtM2Bmy9xWzExI8AWzXaR07Pziv5l
    Bw9yqOMs1VknKeY4jQNJAh57sJ9blp7LILXGBzRs+kssaCBdqYNZoMF+pYqD2jLF27rucSuBF6v
    GSypuczZj8Qi2SwUUPgQjV3+hI56WtHNBaEYe+jJ6yZ0BuKDAcf/9YOLnE4mQtvP4kmH+It89EB
    aimkqKaqJISSyyFq00DAJz00oRKNLPksYFK+ybCWZTPg5FntvVTZYzQx07hoLl4b5FtQSNRDdv3
    keGtyb1jjgF",
    "device_id": "RXDSIOBLZN",
    "sender_key": "uV42E4kJkwkDeXgqBSnej+KJQVlmCWMpO99TTyCrlUI",
    "session_id": "uABZPQHwRZcWiyyc2RMi18BFmO8O9HsFKf+LxvY/6w0"
  },
  "origin_server_ts": 1596484529146,
  "sender": "@user020202:matrix.org",
  "type": "m.room.encrypted",
  "unsigned": {
    "age": 521448
  },
  "event_id": "$LG91xlf7oEmKRuDs8X73RZbk4pfDhhD-CjJf473ipXY",
  "room_id": "!rasnbltJOyNTTHFbCq:matrix.org"
}
```

Protocol analysis
Message types

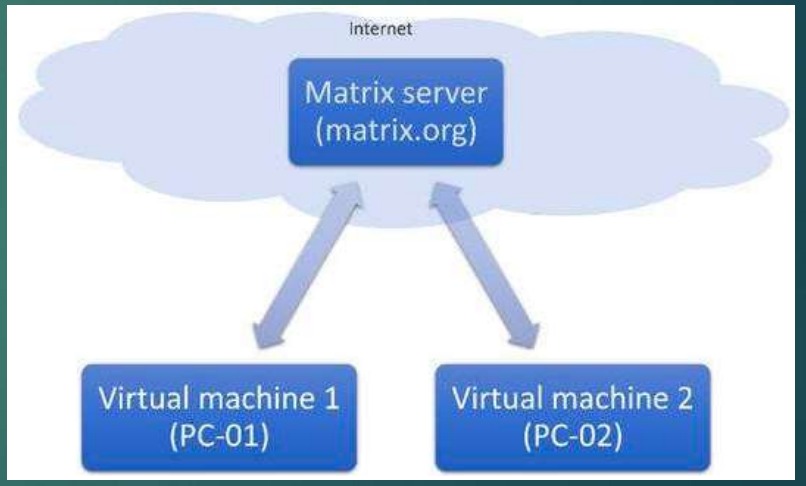
- Text messages (m.text)
- Multimedia messages
  - Video files (m.video)
  - Audio files (m.audio)
  - Images (m.image)
  - Generic files (m.file)

Artifact analysis

- Experiments:
  - Properties of sent and received files
  - "origin_server_ts" timestamp in message events
  - Message events in offline mode
  - Unsigned “age” key-value pair
  - “transaction_id” key-value pair

Artifact analysis Setup

- Two Windows 10 VMs
- Matrix.org server
- Three rooms created
- Dataset for testing



Experiment
Properties of sent and received files

- File properties
- EXIF-data

Experiment "origin_server_ts" timestamp

- Time format
- Timestamp generation
- Date and time of source computer

Experiment
Message events in offline mode

- Temporally event
- Locally generated event identifier
- "origin_server_ts" timestamp based on client date and time
- "origin_server_ts" timestamp updated in final event

Experiment
Message events in offline mode

Experiment
Unsigned “age” key-value pair

- Unsigned key-value pair
- Generated when de message event is downloaded
- Date and time of client doesn’t affect the age-value
- Combining "origin_server_ts” and age value shows date and time the event was downloaded

Experiment "transaction_id" key-value pair

- Unsigned key-value pair
- Only visible in sending client
- Date and time of the client machine

Disk analysis

- Installation
  - No admin rights needed
  - Application: <user>\AppData\Local\riot-desktop\

Disk analysis

- Storage
  - Data: <user>\AppData\Roaming\Riot\
  - LevelDB : AppData\Roaming\Riot\IndexedD/
    - vector_vector_0.indexeddb.leveldb
  - SQLite: AppData\Roaming\Riot\EventStore/
    - “events.db”
  - Cache directory

Conclusion & future work

- A lot of relevant information
  - Timestamps
  - Sending client
  - Servers used
  - Handling of multimedia files
- Future work:
  - Server analysis
  - Encrypted database

Thank you!

DFRWS 2021
VIRTUAL EUROPE

UCD
DUBLIN