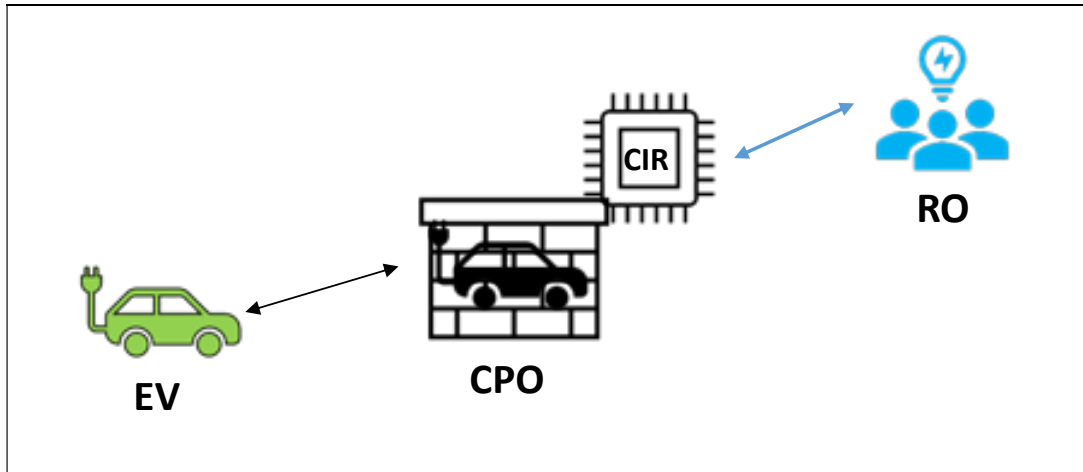


Joint National Conference on Cybersecurity - ITASEC 2026

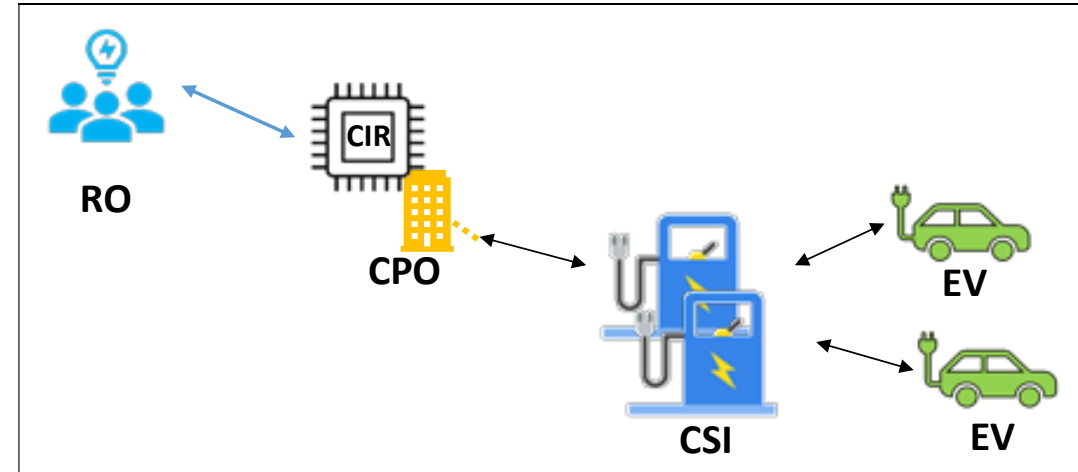
Attack scenarios to charging infrastructure communications



- We are considering two scenarios
 - Private domestic charging infrastructure
 - Private non-domestic charging infrastructure

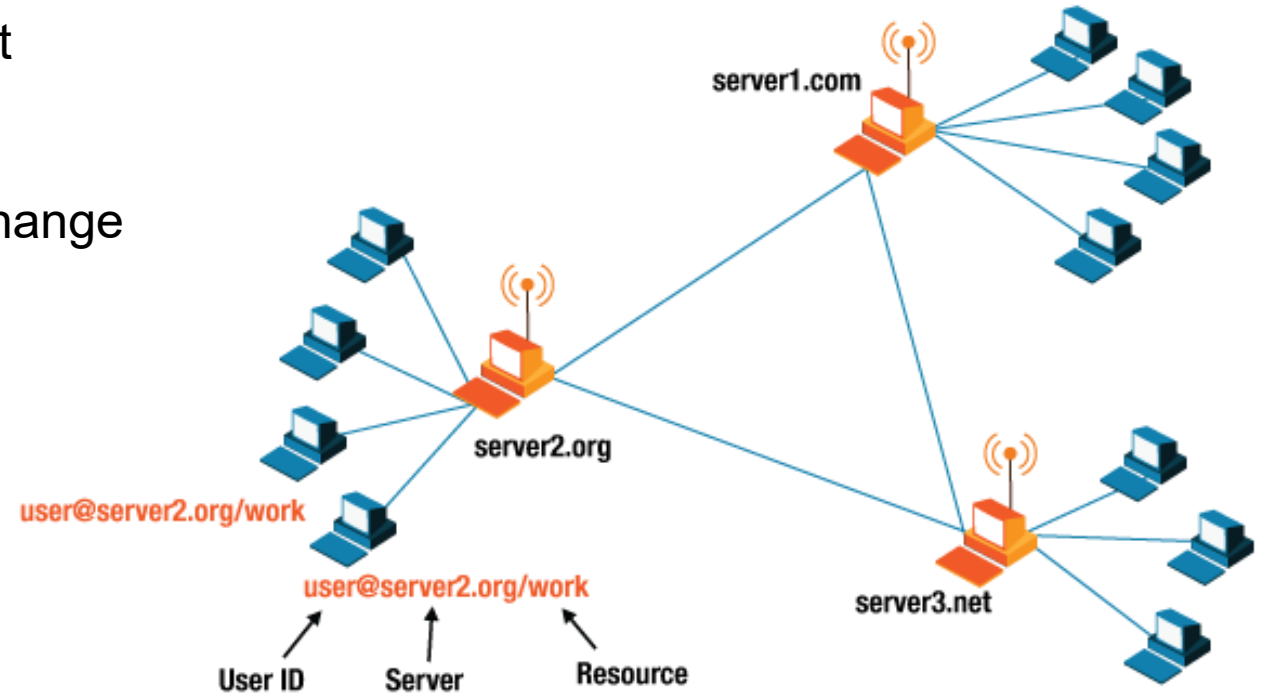


Domestic private charging infrastructure



Non-Domestic private charging infrastructure

- The communication between CIR and RO is made through XMPP
- The eXtensible Messaging and Presence Protocol (XMPP) is XML-based
- It has been standardized with many RFCs
 - RFC 6120: core and messages format
 - RFC 6122: addresses format
 - RFC 7590: TLS support
 - RFC 8600: XMPP for information exchange



- The data exchanged between clients and servers are called «stanzas»
- There are three types of stanzas
 - **Presence**: used for notifying status (online, offline, unavailable)
 - **Message**: used for sending data
 - **IQ** (Info/Query): used for retrieving configurations or information

```
<presence from='cir@xmpp.server' />
```

```
<message to='cir@xmpp.local' type='chat'>  
  <body>  
    <![CDATA[{"UUID": "cmd-9876", "Timetag": 1761501402, "MaximumPower": 1234, "Duration": 1234}]]>  
  </body>  
</message>
```

```
<iq type="get">  
  <query xmlns="jabber:iq:roster" />  
</iq>
```

- There are many supported ways to authenticate to an XMPP server
- ANONYMOUS
- SASL
 - PLAIN
 - SCRAM-SHA-1 o SCRAM-SHA-256
 - DIGEST-MD5
 - EXTERNAL

<p>Server:</p> <pre> <stream:features> <mechanisms xmlns="urn:ietf:params:xml:ns:xmpp-sasl"> <mechanism>SCRAM-SHA-1</mechanism> <mechanism>PLAIN</mechanism> </mechanisms> </stream:features> </pre>	<p>Client:</p> <pre> <auth xmlns="urn:ietf:params:xml:ns:xmpp-sasl" mechanism="SCRAM-SHA-1"> biwsbj1hbGljZSxyPWZ5a28rZDJsYmJnPT0= </auth> </pre>
<p>Server:</p> <pre> <stream:features> <mechanisms xmlns="urn:ietf:params:xml:ns:xmpp-sasl"> <mechanism>EXTERNAL</mechanism> <mechanism>PLAIN</mechanism> </mechanisms> </stream:features> </pre>	<p>Client:</p> <pre> <auth xmlns="urn:ietf:params:xml:ns:xmpp-sasl" mechanism="EXTERNAL"> Zm9vQGV4YW1wbGUuY29t </auth> </pre>

Message family	When / trigger	Primary content	Aim
Cyclic Measures	Periodic (every 20 s)	Aggregated instant active power, available power, time to limiter trip, etc., each with Timetag and quality/invalidity	Provide RO with the measured operating point of the charging infrastructure
Spontaneous Measures	Event-driven	residual time before limiter trip with Timetag/quality	Push time-sensitive measurements to RO when they change/need immediate visibility.
State and Alarms	Event-driven	CSI state (EV connected / no EV / alarm), CIR mode	Inform RO about operational status and alarms.
Acknowledge of RO commands	Immediately upon receiving a command from RO	original command object plus Ack/Nack and Cause	Confirm reception and acceptance/rejection of commands.
Service opt-out / not enabled	When the user decides to stop adhering to the modulation-power service	Message indicating the transition	Notify RO that CIR is no longer available/authorized to provide the modulation service.

Message family	When / trigger	Primary content	Aim
limit max charging power	When there is a need to manage power within limits and/or for flexibility dispatch	Type 1: Maximum Power (W) + Duration (min); Type 2: Maximum Power (W) + Tmax (end timestamp)	Remotely modulate the maximum power the CSI is allowed to draw from the grid.
suspend charging	As needed	Type 1: Duration (min); Type 2: Tmax (end timestamp)	Temporarily stop charging at the CSI under RO supervision.
End of modulation service	When RO decides to terminate the modulation service	End of service notification	Tell CIR that RO stops issuing CMP commands
Acknowledge of measurement packet	After RO receives the measurement ADU	UUID/Timetag/Description and ValueB	Confirm correct reception of CIR measurement packets (lack of ACK triggers CIR retransmissions)

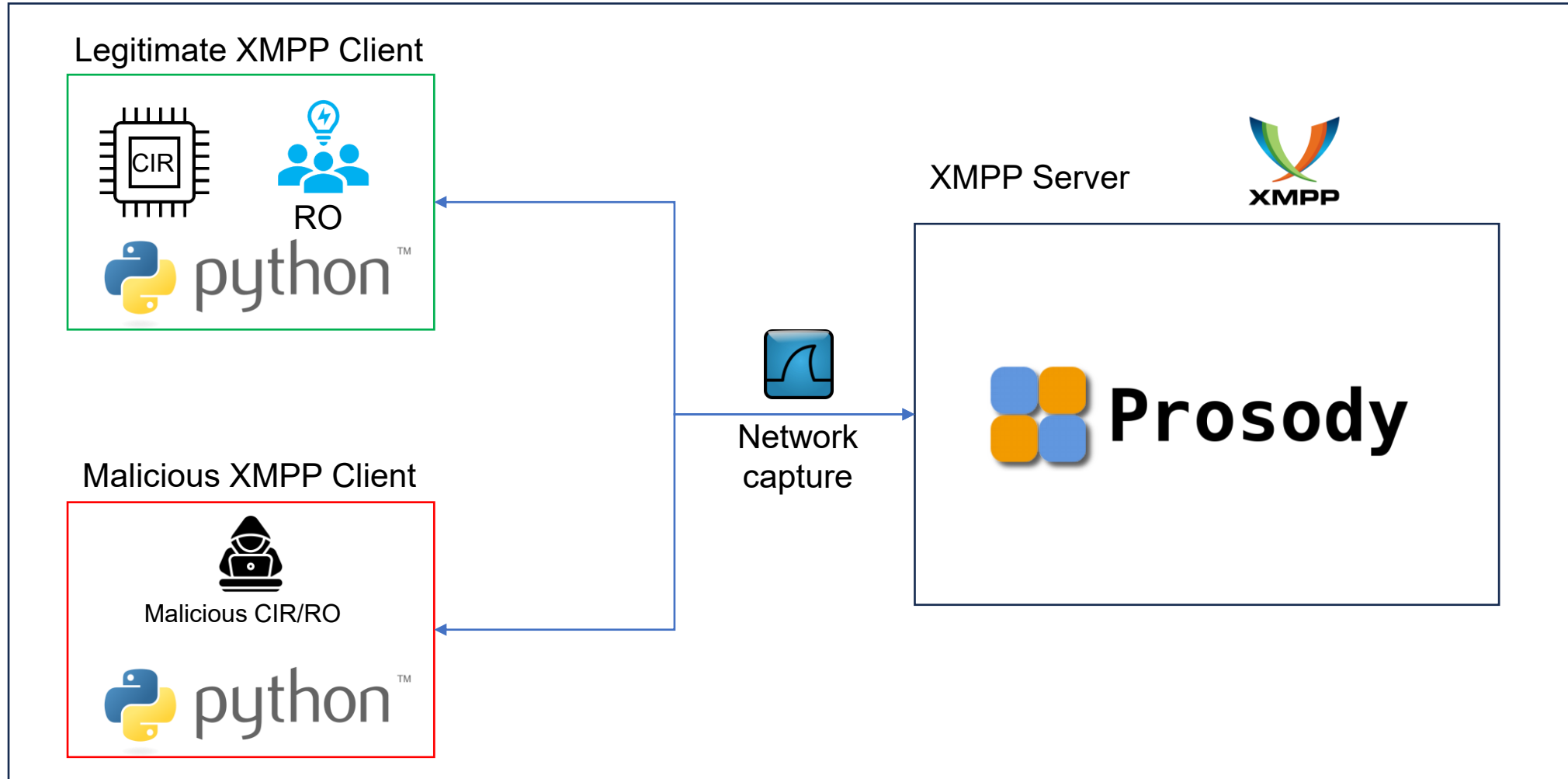
- There are some critical areas in the charging infrastructure standard
 1. In TLS, **Forward Secrecy is not enforced** (it should be)
 2. «It is requested that the servers in the infrastructure be configured in the same way so as to offer the client counterparty (the CIR) exclusively the SASL EXTERNAL mechanism **or, if that is not possible, at least as the preferred option.** »
 3. The CIR should use a certificate to authenticate, however, **username and password are also supported**
- These pitfalls together with intrinsic problems and vulnerabilities related to XMPP, allow us to simulate attack scenarios related to the charging infrastructure

Let us consider some general preconditions necessary for the attacks that we will show

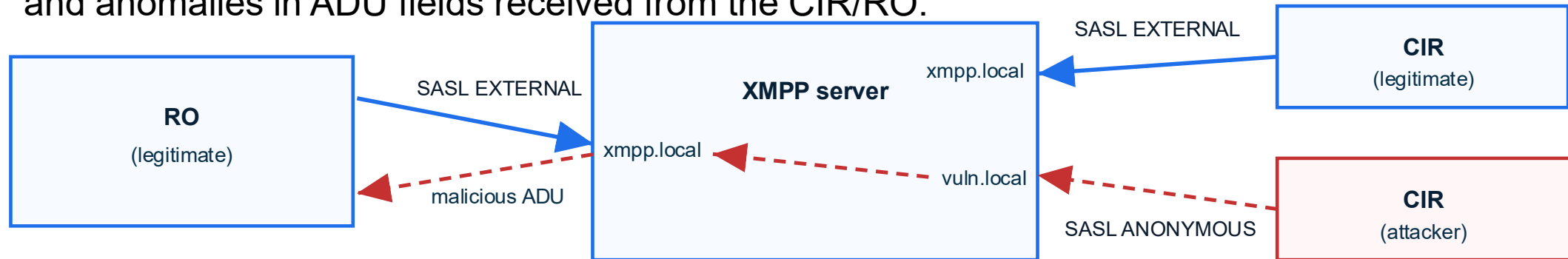
- The attacker obtains the **private key of a client** (CIR/RO)
- The attacker obtains the **private key of the XMPP server**
- The attacker is able to connect to the server **without authentication**
- The attacker is able to connect to the server with **SASL but not of type EXTERNAL**
- The attacker is able to connect to the server using **SASL EXTERNAL**
- The attacker **intercepts a communication** between client and server
- The attacker **compromises a legitimate client** (CIR/RO)

The impact of the attacks varies depending on which parts of the infrastructure are affected. In general, they can be summarized as follows:

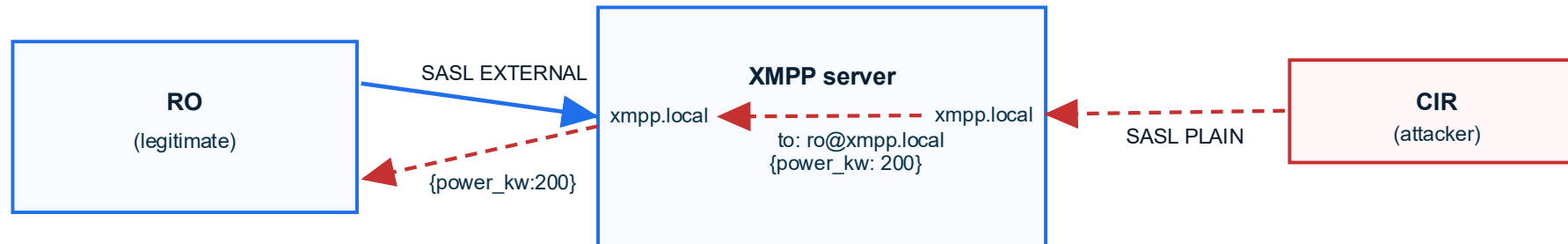
- **Confidentiality:** Occurs when the attacker leaks or retrieves private information such as credentials, ADUs, or other sensitive data. This information can be published for financial gain or used to carry out further attacks (e.g., the attacker intercepts communication between clients)
- **Integrity:** Occurs when the attacker gains the ability to send or inject data into communications between clients, resulting in data poisoning, corruption, or incorrect decisions (e.g., the RO acts on falsified measurements, or the CIR receives tampered commands)
- **Availability:** Occurs when the attacker disrupts the normal functioning of the infrastructure, causing delays or fully preventing the relay of messages (e.g., a Denial-of-Service attack on the XMPP server).



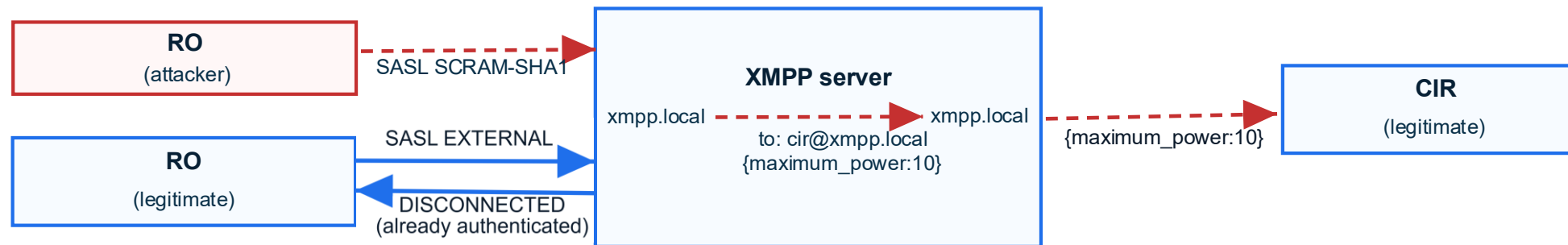
- **Assumptions:** The attacker can authenticate on the network and impersonate a legitimate CIR, or get accredited as a CIR with an RO.
- **Impact:** Integrity: sending falsified or malicious measurements to the RO. Availability: possible compromise of the CIR/RO (malfunctions or overload).
- **Mitigations:** Configure XMPP to allow only trusted mechanisms (e.g., SASL EXTERNAL) and strict validation of client certificates; apply validation checks to the fields of messages received by the RO.
- **AI Features:** Authentication type; client certificate attributes (CA, JID, expiration dates); patterns and anomalies in ADU fields received from the CIR/RO.



- **Assumptions:** The attacker authenticates as, or compromises, a legitimate CIR to send falsified measurement data.
- **Impact:** Integrity: RO decisions based on compromised measurements (e.g., incorrect automated controls).
- **Mitigations:** Strict RO-side validation of measurements (range and plausibility, temporal consistency checks, cross-checking with other sources); rate limiting; flag unusual patterns.
- **AI Features:** Features extracted from ADUs (field values, statistical distribution, subtle deviations from benign behavior); anomaly-detection models trained on large datasets of legitimate measurements



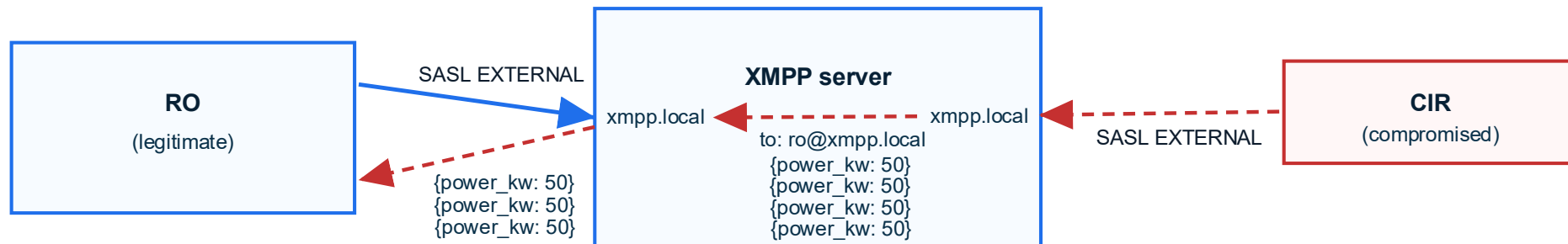
- **Assumptions:** The attacker authenticates to the server and presents as an RO, receiving measurements from CIRs and sending commands.
- **Impact:** Availability: malicious commands can suspend or damage CIRs. Integrity: manipulated data circulates in the network and influences its behavior.
- **Mitigations:** Strict authentication validation on the XMPP server; CIR-side checks on authorization and plausibility of received commands; access control and logging of RO actions.
- **AI Features:** Authentication metadata (method, certificate, JID); patterns and content of command-type ADUs sent by the RO; anomalies in command values or frequency.



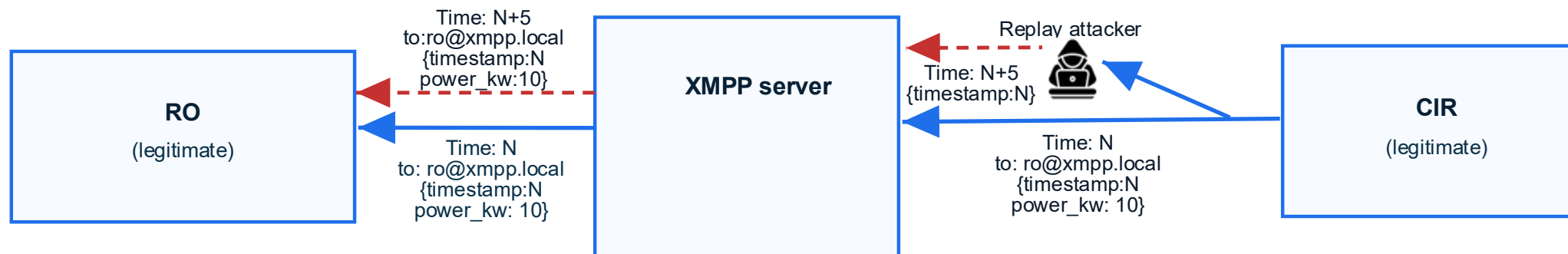
- **Assumptions:** The attacker manages to intercept or insert themselves into the communication between XMPP clients and server.
- **Impact:** Confidentiality: exposure of data in transit. Integrity: if the attacker manipulates messages, integrity is also compromised.
- **Mitigations:** Enforce modern cipher suites and forward secrecy. Certificate validation, monitoring, and detection of anomalous certificates.
- **AI Features:** Transport metrics (latency, inter-arrival time, packet size, TTL), changes in TCP/IP patterns; if manipulation is possible, also ADU payload features (semantic inconsistencies).



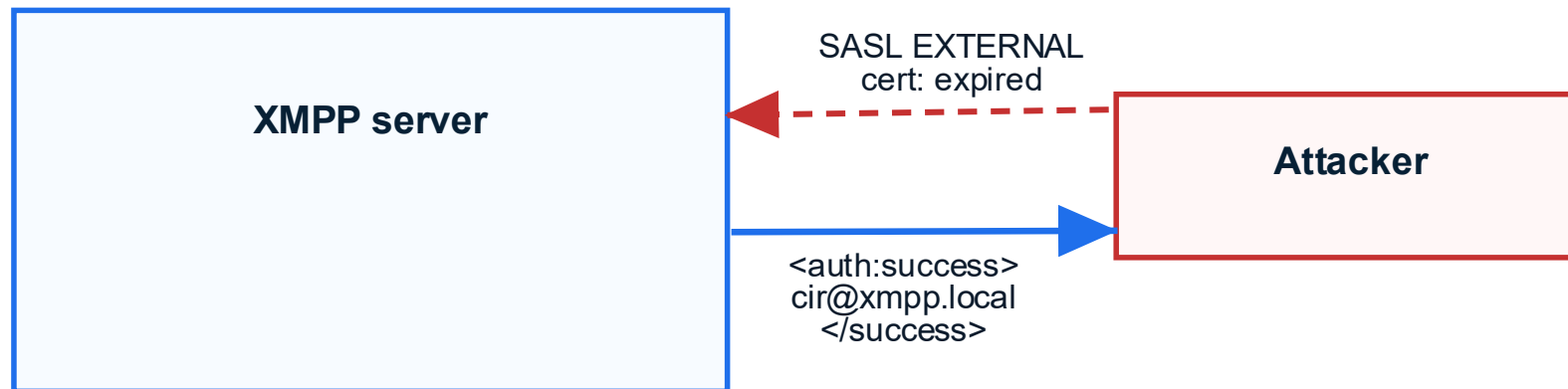
- **Assumptions:** The attacker can establish connections to the XMPP server; whether authenticated or not, they can generate malicious traffic or overload services/clients.
- **Impact:** Availability: degradation or interruption of the XMPP service; CIR or RO unreachable.
- **Mitigations:** Rate limiting; per-client payload limits; maximum simultaneous connections per JID/IP.
- **AI Features:** TCP/flow metrics: packet volume, inter-arrival time, packet size, connection duration, concurrent-connection patterns.



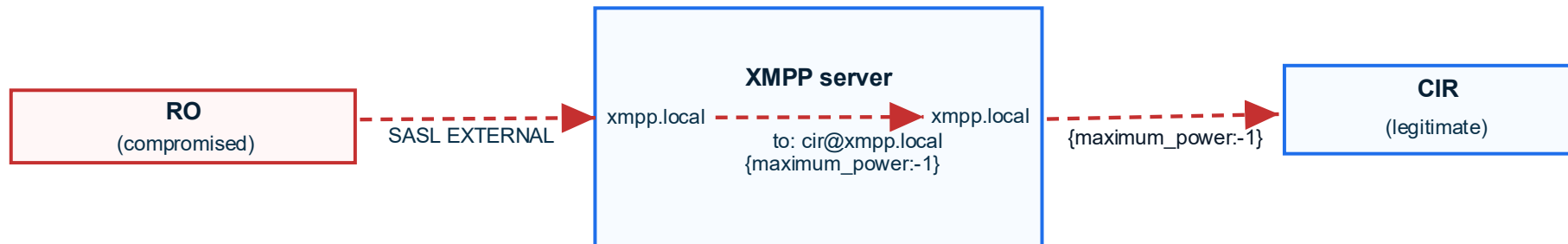
- **Assumptions:** The attacker intercepts and retransmits legitimate messages; more effective if they can alter messages.
- **Impact:** Integrity: reapplying data or commands causes undesired effects; temporal consistency compromised.
- **Mitigations:** Validate timestamps and an acceptance time window on the receiving side.
- **AI Features:** Timestamp analysis in ADU payloads; counting identical messages; network metrics similar to MITM (latency, TTL) to identify anomalous retransmissions.



- **Assumptions:** The attacker can connect and present a certificate; the attack succeeds if the XMPP server does not properly validate the certificate.
- **Impact:** Integrity: the attacker can authenticate as a legitimate entity, compromising communications and data.
- **Mitigations:** Strict certificate validation (expiration, trust chain, revocation checks, and cross-checks on the issuing CA).
- **AI Features:** Inspection of the presented certificate fields (issuer, CA, related JIDs, validity dates); patterns of anomalous certificates or uncommon CAs.



- **Assumptions:** The attacker has compromised a real RO.
- **Impact:** Integrity: sending malicious commands/messages into the network; possible effects on CIR operation.
- **Mitigations:** Keep servers and RO free of known vulnerabilities (patching, hardening); monitor RO integrity.
- **AI Features:** If compromise occurs via the network: inspect ADU payloads originating from the RO for anomalous commands; if compromised locally, analyze behavioral patterns and anomalies in ADU fields/telemetry.



For future work, we consider the following directions:

- Studying and building scenarios with **chains of vulnerabilities**
- Running the simulations to **capture network traffic**, generating a syntetic dataset
- Perform a **feature engineering** study to identify meaningful statistics in the network traffic that can aid in detecting attacks
- Create a model for the **AI-based detection** of attacks against the infrastructure

Overall future work aims to create a consistent set of scenarios that can be used to carry out realistic simulations that are used to build protections against attacks

With this work we provide:

- **A study of 7 preconditions** that can lead to a compromise of the infrastructure
- **A study and simulation of 8 attack scenarios**, showing assumptions, impact, mitigations and potential features to perform AI-based detection

These contributions can be used to:

- Check if a real charging infrastructure is vulnerable
- Improve existing defenses
- Simulate realistic attack scenarios
- Build datasets
- Improve the standard to take into account these scenarios

Thank you for the attention

Lorenzo Pisu, Davide Maiorca, Giorgio Fumera, Giorgio Giacinto

{name.surname}@unica.it