Access Control and Availability Vulnerabilities in the ISO/IEC 61850 Substation Automation Protocol

James Wright
Dr. Stephen Wolthusen
Information Security Group
Royal Holloway University of London
james.wright.2015@rhul.ac.uk
&
stephen.wolthusen@rhul.ac.uk

October 10, 2016

Presentation Contents

Table of Contents

Defining our Problem

- Does the IEC61850 standard meet the security promises laid out in its specification of access control and availability?

Defining our Problem

- Does the IEC61850 standard meet the security promises laid out in its specification of access control and availability?
- If there are omissions, can they be exploited?

Defining our Problem

- Does the IEC61850 standard meet the security promises laid out in its specification of access control and availability?
- If there are omissions, can they be exploited?
- Can these attacks still occur in a fully compliant implementation of the protocol?

The Protocol Problem

- The assumption in the research community is that the communication and security protocols that Smart Grids will operate on are secure. Whilst each protocol makes certain security promises, no one seems to have verified if these statements are true throughout their specification.

The Protocol Problem

- The assumption in the research community is that the communication and security protocols that Smart Grids will operate on are secure. Whilst each protocol makes certain security promises, no one seems to have verified if these statements are true throughout their specification.
- No one has checked if security promises come into conflict with the quality of service requirements.

The Protocol Problem

- The assumption in the research community is that the communication and security protocols that Smart Grids will operate on are secure. Whilst each protocol makes certain security promises, no one seems to have verified if these statements are true throughout their specification.
- No one has checked if security promises come into conflict with the quality of service requirements.
- Making sure that these statements are true could prevent some theorised attacks.

The Protocol Problem

- The assumption in the research community is that the communication and security protocols that Smart Grids will operate on are secure. Whilst each protocol makes certain security promises, no one seems to have verified if these statements are true throughout their specification.
- No one has checked if security promises come into conflict with the quality of service requirements.
- Making sure that these statements are true could prevent some theorised attacks.
- Currently looking at IEC61850 in isolation. The explicit security promise of access control, availability, and data integrity against transmission error.

Table of Contents

Related Works

- Attack taxonomies for generic Smart Grid systems. Some specific to IEC61850.

Related Works

- Attack taxonomies for generic Smart Grid systems. Some specific to IEC61850.
- Securing older SCADA protocols (e.g. DNP3).

Related Works

- Attack taxonomies for generic Smart Grid systems. Some specific to IEC61850.
- Securing older SCADA protocols (e.g. DNP3).
- Use of finite-state machines in security.

Related Works

- Attack taxonomies for generic Smart Grid systems. Some specific to IEC61850.
- Securing older SCADA protocols (e.g. DNP3).
- Use of finite-state machines in security.
- Use of Context-free grammar for security.

Attacks on GOOSE Messages

- Hoyos *et al.* proposed a GOOSE spoofing attack

Attacks on GOOSE Messages

- Hoyos *et al.* proposed a GOOSE spoofing attack
- Kush *et al.*. They developed a denial of service

Table of Contents

The Premise

The attack allows the attacker (who has no credentials) to intercept the login attempt of a legitimate user and steal their successful login attempt. It is based upon the two party association model as described in IEC61850-7-2 section 8.3.

The Premise

The attack allows the attacker (who has no credentials) to intercept the login attempt of a legitimate user and steal their successful login attempt. It is based upon the two party association model as described in IEC61850-7-2 section 8.3.

- The client sends a legitimate login request to their own personal LN server view.

The Premise

The attack allows the attacker (who has no credentials) to intercept the login attempt of a legitimate user and steal their successful login attempt. It is based upon the two party association model as described in IEC61850-7-2 section 8.3.

- The client sends a legitimate login request to their own personal LN server view.
- The adversary sees the traffic going through his intercept.

The Premise

The attack allows the attacker (who has no credentials) to intercept the login attempt of a legitimate user and steal their successful login attempt. It is based upon the two party association model as described in IEC61850-7-2 section 8.3.

- The client sends a legitimate login request to their own personal LN server view.
- The adversary sees the traffic going through his intercept.
- Seeing this, the adversary sends a garbage login to their own login view.

The Premise

The attack allows the attacker (who has no credentials) to intercept the login attempt of a legitimate user and steal their successful login attempt. It is based upon the two party association model as described in IEC61850-7-2 section 8.3.

- The client sends a legitimate login request to their own personal LN server view.
- The adversary sees the traffic going through his intercept.
- Seeing this, the adversary sends a garbage login to their own login view.
- When the client's view responds with the login credentials, the attacker intercepts the authentication ID.

The Premise

The attack allows the attacker (who has no credentials) to intercept the login attempt of a legitimate user and steal their successful login attempt. It is based upon the two party association model as described in IEC61850-7-2 section 8.3.

- The client sends a legitimate login request to their own personal LN server view.
- The adversary sees the traffic going through his intercept.
- Seeing this, the adversary sends a garbage login to their own login view.
- When the client's view responds with the login credentials, the attacker intercepts the authentication ID.
- The adversary forwards their failed login attempt message to the client.

The Adversary Rules

- The adversary can see all packets passing between the client and the LN server

The Adversary Rules

- The adversary can see all packets passing between the client and the LN server
- The adversary cannot send any message that they have not already seen before him

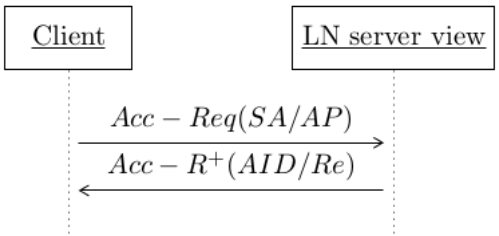
The Adversary Rules

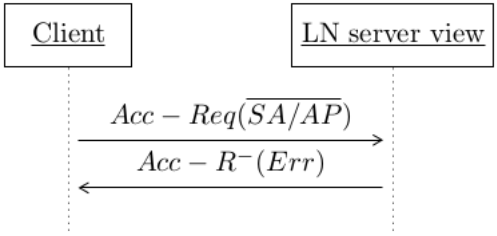
- The adversary can see all packets passing between the client and the LN server
- The adversary cannot send any message that they have not already seen before him
- The adversary has no buffer on messages they have seen. They have to send the message directly after seeing.

The Adversary Rules

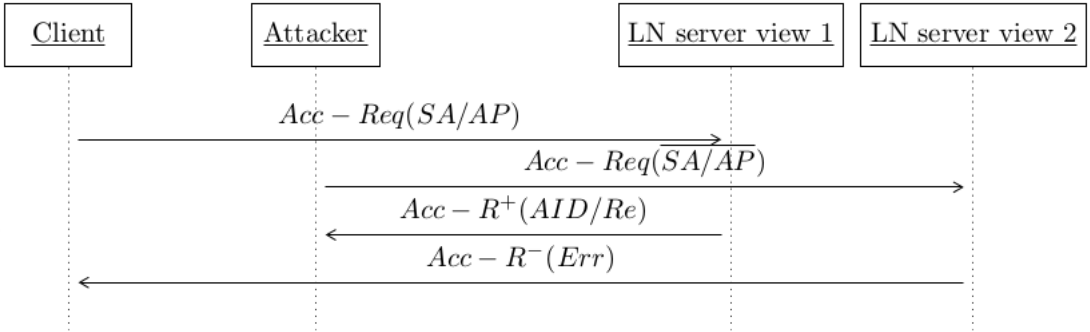
- The adversary can see all packets passing between the client and the LN server
- The adversary cannot send any message that they have not already seen before him
- The adversary has no buffer on messages they have seen. They have to send the message directly after seeing.
- The adversary can forward and intercept packets

Session diagrams for legitmate messages





attack session diagram



Formal Grammar

Start variable: S

Terminals: $Acc - Req(), SA/AP, Acc - R^{+}(AID/Re), \overline{SA/AP}, Acc - R^{-}(Err)$

- $S \rightarrow TATV|TWTW|TV|TW$
- $R \rightarrow Acc - Req()$
- $V \rightarrow \overline{SA/AP}Acc - R^{-}(Err)$
- $W \rightarrow SA/APAcc - R^{+}(AID/Re)$
- $T \rightarrow RU$
- $U \rightarrow VT|\epsilon$
- $A \rightarrow W|RVW|RWV$

The Legitimate Message Rules

- A login attempt for one access view must be completed before a second login view can be attempted

The Legitimate Message Rules

- A login attempt for one access view must be completed before a second login view can be attempted
- There can only be two successful attempts per run

The Legitimate Message Rules

- A login attempt for one access view must be completed before a second login view can be attempted
- There can only be two successful attempts per run
- An infinite number of failed attempts can be made before the first successful message and before the final message.

Legitimate Message Forms

- $(Acc - Req()\overline{SA/AP}Acc - R^{-}(Err))^{n}\ Acc - Req()SA/APAcc - R^{+}(AID/Re)$
  $(Acc - Req()\overline{SA/AP}Acc - R^{-}(Err))^{n}\ Acc - Req()SA/APAcc - R^{+}(AID/Re)$
- $(Acc - Req()\overline{SA/AP}Acc - R^{-}(Err))^{n}\ Acc - Req()SA/APAcc - R^{+}(AID/Re)$
  $(Acc - Req()\overline{SA/AP}Acc - R^{-}(Err))^{n}$
- $(Acc - Req()\overline{SA/AP}Acc - R^{-}(Err))^{n}\ Acc - Req()SA/APAcc - R^{+}(AID/Re)$
- $(Acc - Req()\overline{SA/AP}Acc - R^{-}(Err))^{n}$

The Undesired Message Rules

- The adversary can only duplicate a message they have already seen

The Undesired Message Rules

- The adversary can only duplicate a message they have already seen
- The adversary '$Acc - Req()$' must come before the clients 'AP/SA', this is to make sure it passes through the C_1C_2 state of the two user automata.

The Undesired Message Rules

- The adversary can only duplicate a message they have already seen
- The adversary '$Acc - Req()$' must come before the clients 'AP/SA', this is to make sure it passes through the C_1C_2 state of the two user automata.
- The adversary can only send $\overline{SA/AP}$ credentials, to make sure it ends up in the state they desire (S_1A_2 or A_1S_2)

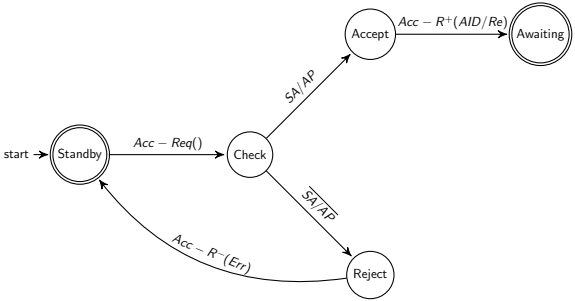
The Undesired Message Rules

- The adversary can only duplicate a message they have already seen
- The adversary '$Acc - Req()$' must come before the clients 'AP/SA', this is to make sure it passes through the C_1C_2 state of the two user automata.
- The adversary can only send $\overline{SA/AP}$ credentials, to make sure it ends up in the state they desire (S_1A_2 or A_1S_2)
- The legitimate user can't login after the adversary has intercepted their credentials.

Undesired Message Forms

- $(Acc - Req()\overline{SA/AP}Acc - R^{-}(Err))^{n}$
  $Acc - Req()Acc - Req()\overline{SA/AP}Acc - R^{-}(Err)SA/APAcc - R^{+}(AID/Re)$
  $(Acc - Req()\overline{SA/AP}Acc - R^{-}(Err))^{n}$
- $(Acc - Req()\overline{SA/AP}Acc - R^{-}(Err))^{n}$
  $Acc - Req()Acc - Req()SA/APAcc - R^{+}(AID/Re)\overline{SA/AP}Acc - R^{-}(Err)$
  $(Acc - Req()\overline{SA/AP}Acc - R^{-}(Err))^{n}$

One User Automata



Two User Automata

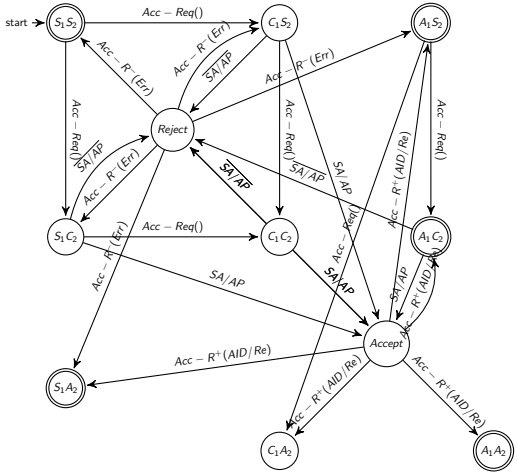


Table of Contents

The Premise

- An attack using GOOSE or GSSE messages, described in IEC61850-7-2, can be used to create a DoS attack against the communications network

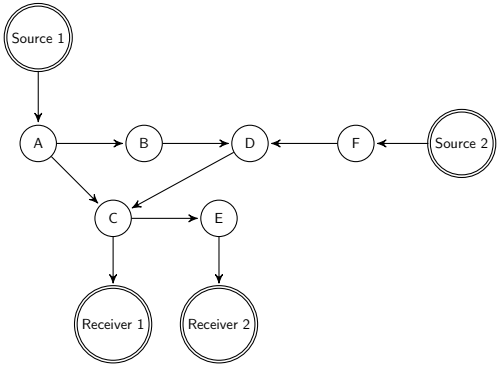
The Premise

- An attack using GOOSE or GSSE messages, described in IEC61850-7-2, can be used to create a DoS attack against the communications network
- The attacker degrades the performance of packet transfer between IED's below the acceptable QoS latency, by sending messages that connects additional subscribers or topological branches to a LN's generic substation event subscriber list.

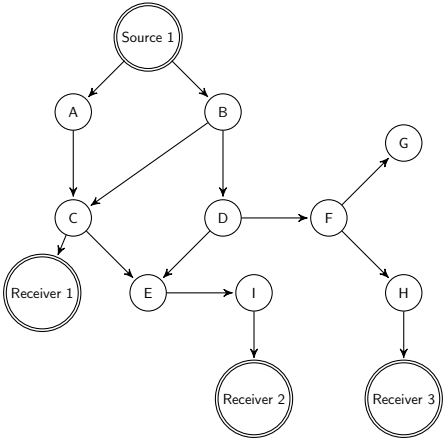
The Premise

- An attack using GOOSE or GSSE messages, described in IEC61850-7-2, can be used to create a DoS attack against the communications network
- The attacker degrades the performance of packet transfer between IED's below the acceptable QoS latency, by sending messages that connects additional subscribers or topological branches to a LN's generic substation event subscriber list.
- It is assumed that the GSE model has implemented on PIM multicast framework that has been applied to a network substrate that supports it.

Sparse Topology



Dense Topology



The attack

- The adversary model is the same as the one for the access control attack, except the adversary has a buffer so they are not required to send messages they have discerned immediately.

The attack

- The adversary model is the same as the one for the access control attack, except the adversary has a buffer so they are not required to send messages they have discerned immediately.
- The adversary must perform some passive surveillance on the communications network.

The attack

- The adversary model is the same as the one for the access control attack, except the adversary has a buffer so they are not required to send messages they have discerned immediately.
- The adversary must perform some passive surveillance on the communications network.
- The adversary sends a PIM message to add the branch/LN to the subscriber list.

The attack

- The adversary model is the same as the one for the access control attack, except the adversary has a buffer so they are not required to send messages they have discerned immediately.
- The adversary must perform some passive surveillance on the communications network.
- The adversary sends a PIM message to add the branch/LN to the subscriber list.
- The next time the publisher LN sends out a GOOSE/GSSE message to the network the LNs that have been maliciously subscribed to the network will receive messages they weren't expecting.

Workflow Amplifcation Factor Equations

$$\text{Amplification factor}_{\text{GOOSE}} = \frac{A + \text{length of data set} + \text{data set}}{B + C} \quad (1)$$

Workflow Amplifcation Factor Equations

$$\text{Amplification factor}_{\text{GOOSE}} = \frac{A + \text{length of data set} + \text{data set}}{B + C} \quad (1)$$

$$\text{Amplification factor}_{\text{GSSE}} = \frac{D + (2 * \text{length of data set})}{B + C} \quad (2)$$

Workflow Amplifcation Factors

	AF_{GOOSE}	AF_{GSSE}
Case 1	3.96	3.63
Case 2	23.75	22.14
Case 3	11.87	11.07

Table of Contents

Future work

- Further study IEC61850 and IEC62351, as well how the two interact with each other.

Future work

- Further study IEC61850 and IEC62351, as well how the two interact with each other.
- Develop more attacks in IEC61850 (Privilege escalation, credential swapping, DoS via packet amplification, etc) using alternative modelling techniques, such as queuing theory and process algebra.

Future work

- Further study IEC61850 and IEC62351, as well how the two interact with each other.
- Develop more attacks in IEC61850 (Privilege escalation, credential swapping, DoS via packet amplification, etc) using alternative modelling techniques, such as queuing theory and process algebra.
- See if these attacks can still be executed in IEC62351.

Future work

- Further study IEC61850 and IEC62351, as well how the two interact with each other.
- Develop more attacks in IEC61850 (Privilege escalation, credential swapping, DoS via packet amplification, etc) using alternative modelling techniques, such as queuing theory and process algebra.
- See if these attacks can still be executed in IEC62351.
- See if undesired actions can be executed that would cause damage to the power grid.

Questions?