ELECTRIC POWER
RESEARCH INSTITUTE

Attack Trees for Selected Electric Sector High Risk Failure Scenarios
NESCOR

Version 1.0

September 2013

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

Slide Set Background and Purpose

- Contains key results from NESCOR* document: “Analysis of Selected Electric Sector High Risk Failure Scenarios” [2]
  - Failure scenarios selected from the prior NESCOR document “Electric Sector Failure Scenarios and Impact Analyses” [1]
- PowerPoint format supports:
  - Tailoring of information by utilities
  - Use of information in a meeting setting

*NESCOR – National Electric Sector Cybersecurity Organization Resource

Overview of Slide Set

- Attack tree notation
- Attack trees for selected failure scenarios, with
  - Short text descriptions
  - Relevant architecture diagrams for some scenarios
- Common sub trees
  - These are modular fragments of attack trees, reused within failure scenario trees
  - Attack sub trees with short text descriptions
- Acronym list

Selected Failure Scenarios

- **AMI.1**[*] - *Mass Meter Disconnect*
- **AMI.9** - *Invalid Disconnect Messages to Meters Impact Customers and Utility*
- **AMI.12** - *Improper Firewall Configuration Exposes Customer Data*
- **AMI.14** - *Breach of Cellular Provider's Network Exposes AMI Access*
- **AMI.16** - *Compromised Head end Allows Impersonation of CA*
- **AMI.27** - *Reverse Engineering of AMI Equipment Allows Unauthorized Mass Control*
- **AMI.29** - *Unauthorized Device Acquires HAN Access and Steals PII*
- **AMI.32**[*] **-** *Power Stolen by Reconfiguring Meter via Optical Port*
- **DGM.11**[*] - *Threat Agent Triggers Blackout via Remote Access to Distribution System*
- **DR.1** - *Blocked DR Messages Result in Increased Prices or Outages*
- **DR.4** - *Improper DRAS Configuration Causes Inappropriate DR Messages*

[*] For these scenarios, a detailed text format analysis can be found in [2]. For all scenarios, a brief text format analysis can be found in [1].

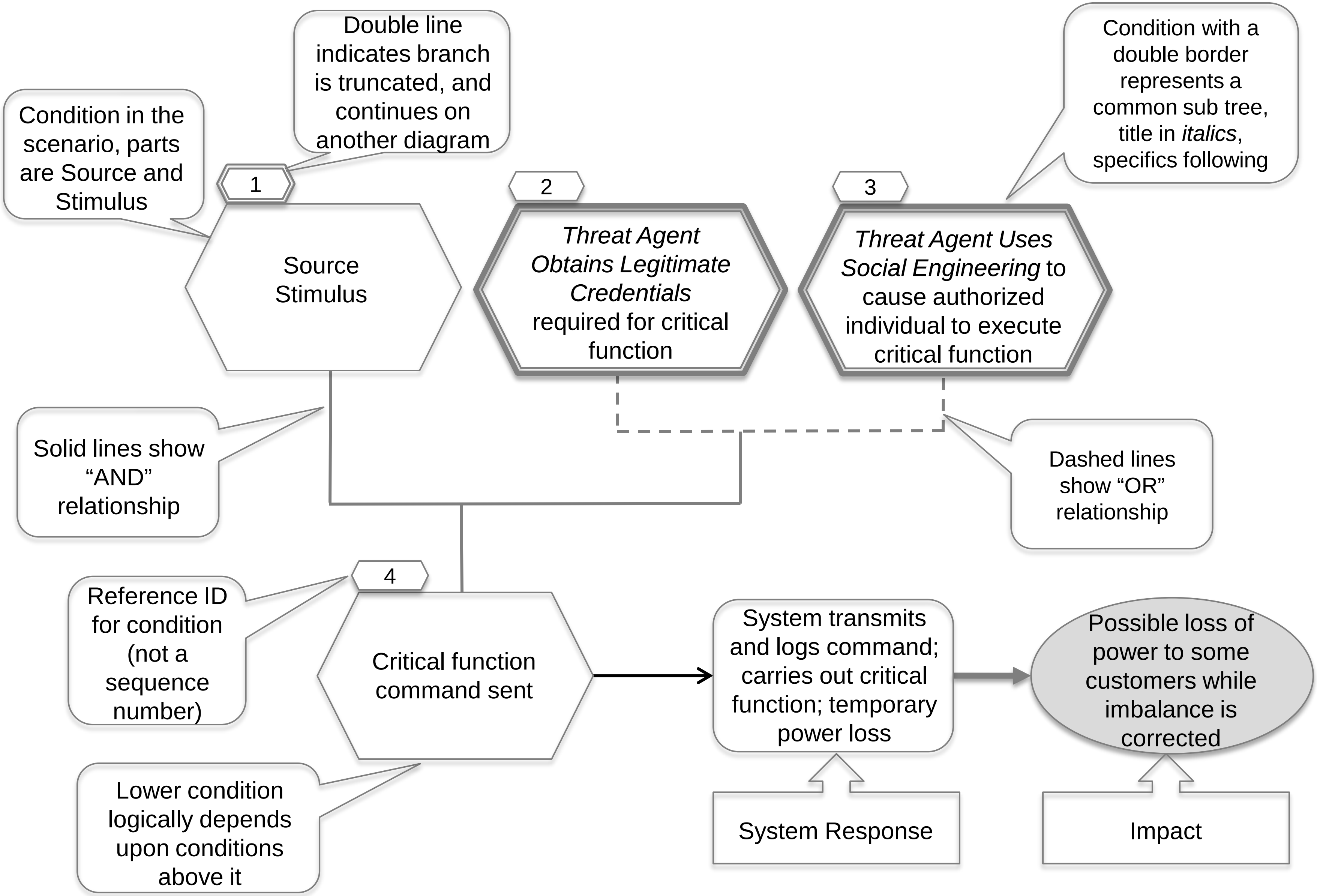
Attack Tree Notation Quick Start

- The generic example on the next slide illustrates how to read an attack tree.
- The tree is shown on each slide, with truncated branches represented by double lines around the numbered small hexagons. These branches are then shown on another slide.
- The *common sub trees* referenced in the attack trees are fragments of attack trees which were found to be repeated across many different trees as well as within attack trees.
  - More appropriate to present them once, and then invoke them using relevant references.
  - The large hexagon that names the common sub tree has a double outline.
- *Common mitigations* are in italics, followed by specifics for the failure scenario.

Common Sub Trees

- Threat Agent Gains Capability to Reconfigure <firewall>
- Threat Agent Blocks Wireless Communication Channel Connecting <x and y>
- Authorized Employee Brings Malware into <system or network>
- Threat Agent Obtains Legitimate Credentials for <system or function>
- Threat Agent Uses Social Engineering to <desired outcome>
- Threat Agent Finds Firewall Gap <specific firewall>
- Threat Agent Steals <file>
- Threat Agent Gains Access to <network>

Attack Tree Notation Icons



Condition in the scenario, parts are Source and Stimulus

Double line indicates branch is truncated, and continues on another diagram

1

Source Stimulus

2

Threat Agent Obtains Legitimate Credentials required for critical function

3

Threat Agent Uses Social Engineering to cause authorized individual to execute critical function

Condition with a double border represents a common sub tree, title in *italics*, specifics following

Solid lines show "AND" relationship

Dashed lines show "OR" relationship

Reference ID for condition (not a sequence number)

4

Critical function command sent

System transmits and logs command; carries out critical function; temporary power loss

Possible loss of power to some customers while imbalance is corrected

Lower condition logically depends upon conditions above it

System Response

Impact

AMI.1 Mass Meter Remote Disconnect by Authorized Individual

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

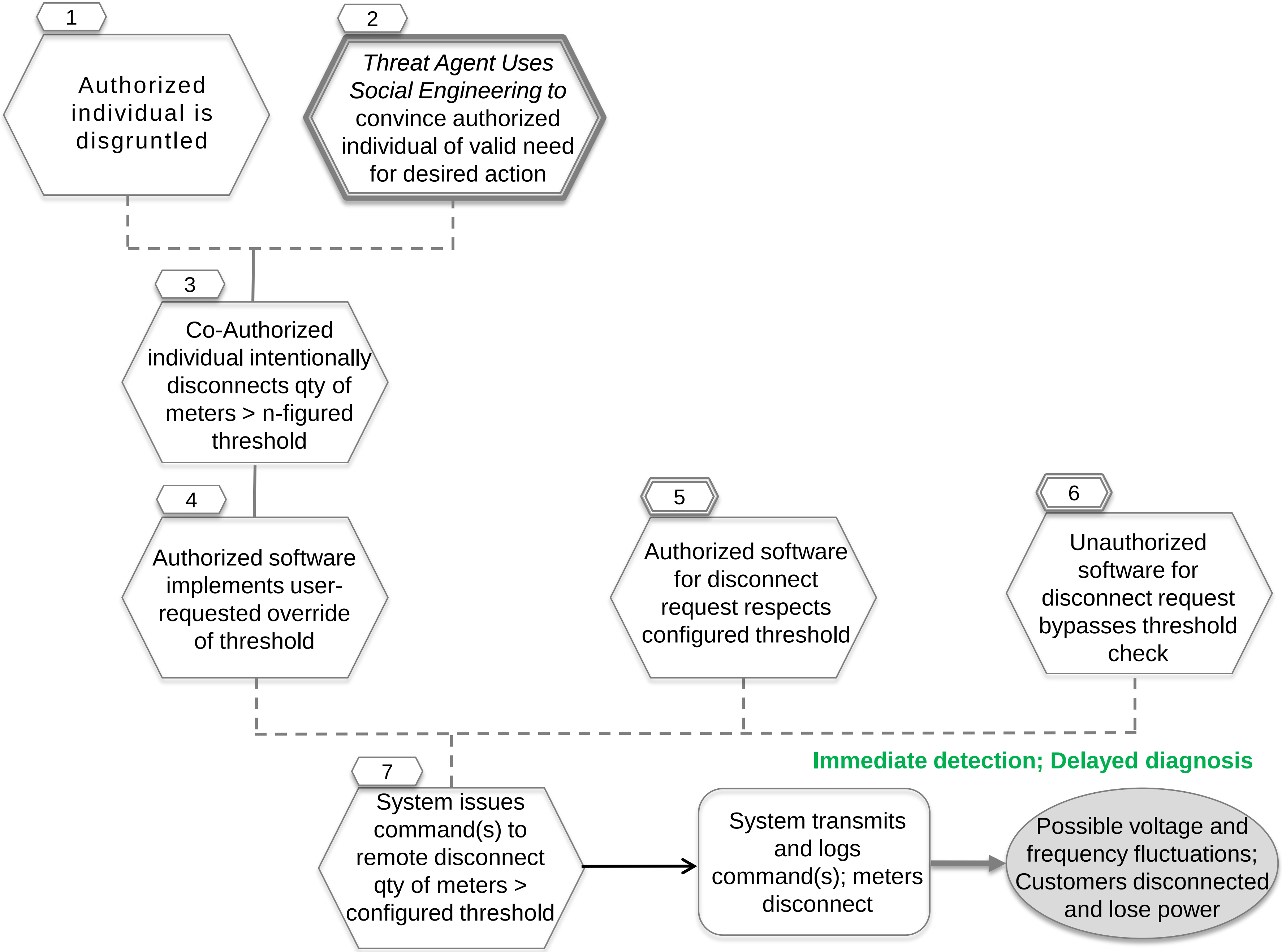
Description

An authorized individual (defined as an individual who legitimately has privileges to remotely disconnect meters) issues a command or commands that causes disconnect of a massive number of meters within a short time period.

Assumptions

- Two stage disconnect process – request and implement
- Authentication and roles in place for disconnect request
- Implement stage warns when meter quantity threshold exceeded (stronger enforcement not assumed)
- Implement stage verifies business rules such as critical service, billing status
- Remote install of software requires VPN connection and strong authentication
- Requests for disconnect are logged with user name, log strongly protected.

AMI.1 Authorized Individual Issues Unauthorized Mass Remote Disconnect (1/3)



1 Authorized individual is disgruntled

2 *Threat Agent Uses Social Engineering to* convince authorized individual of valid need for desired action

3 Co-Authorized individual intentionally disconnects qty of meters > n-figured threshold

4 Authorized software implements user-requested override of threshold

5 Authorized software for disconnect request respects configured threshold

6 Unauthorized software for disconnect request bypasses threshold check

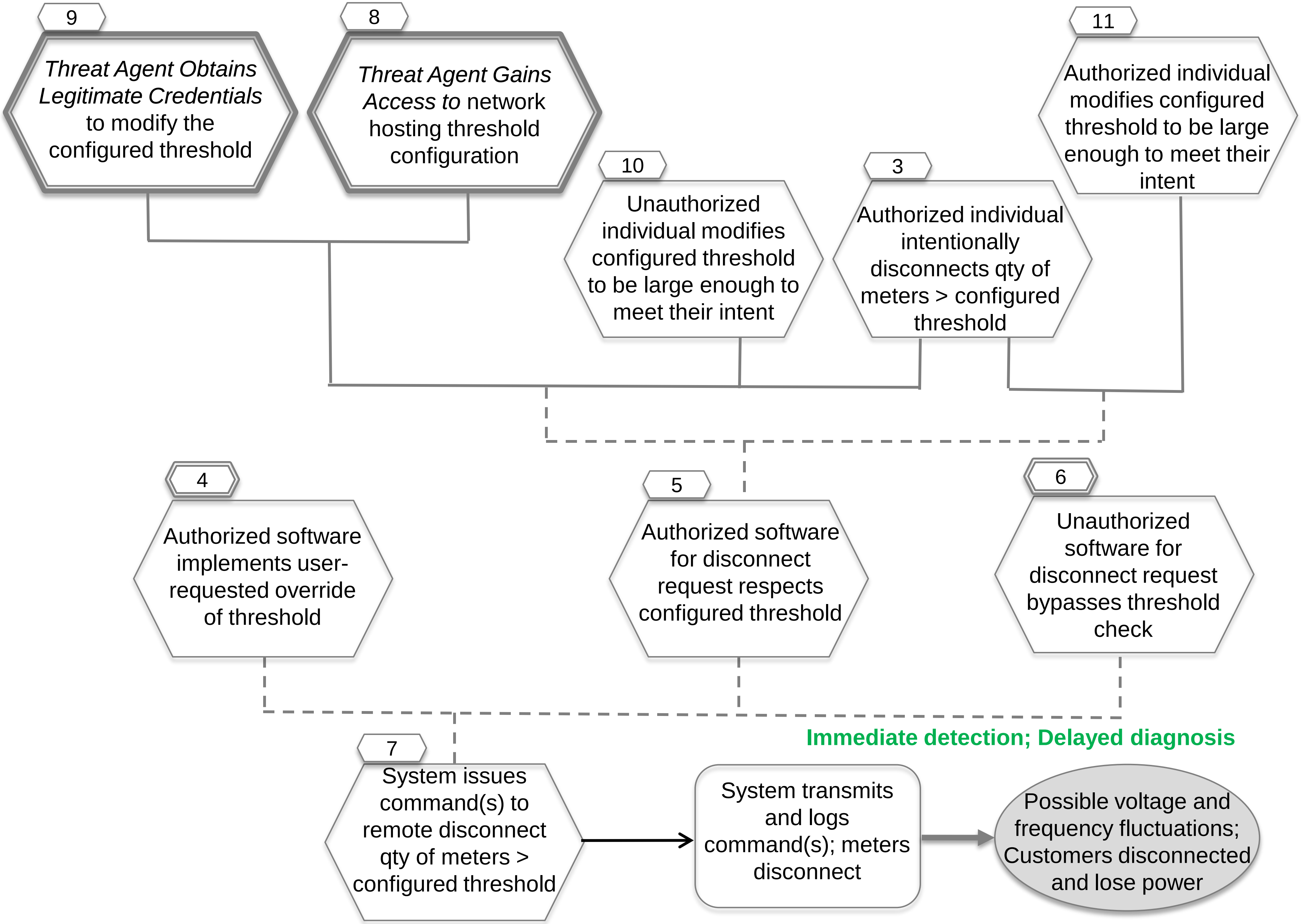
7 System issues command(s) to remote disconnect qty of meters > configured threshold

System transmits and logs command(s); meters disconnect

Possible voltage and frequency fluctuations; Customers disconnected and lose power

Immediate detection; Delayed diagnosis

AMI.1 Authorized Individual Issues Unauthorized Mass Remote Disconnect (2/3)



9 *Threat Agent Obtains Legitimate Credentials* to modify the configured threshold

8 *Threat Agent Gains Access to* network hosting threshold configuration

10 Unauthorized individual modifies configured threshold to be large enough to meet their intent

3 Authorized individual intentionally disconnects qty of meters > configured threshold

11 Authorized individual modifies configured threshold to be large enough to meet their intent

4 Authorized software implements user-requested override of threshold

5 Authorized software for disconnect request respects configured threshold

6 Unauthorized software for disconnect request bypasses threshold check

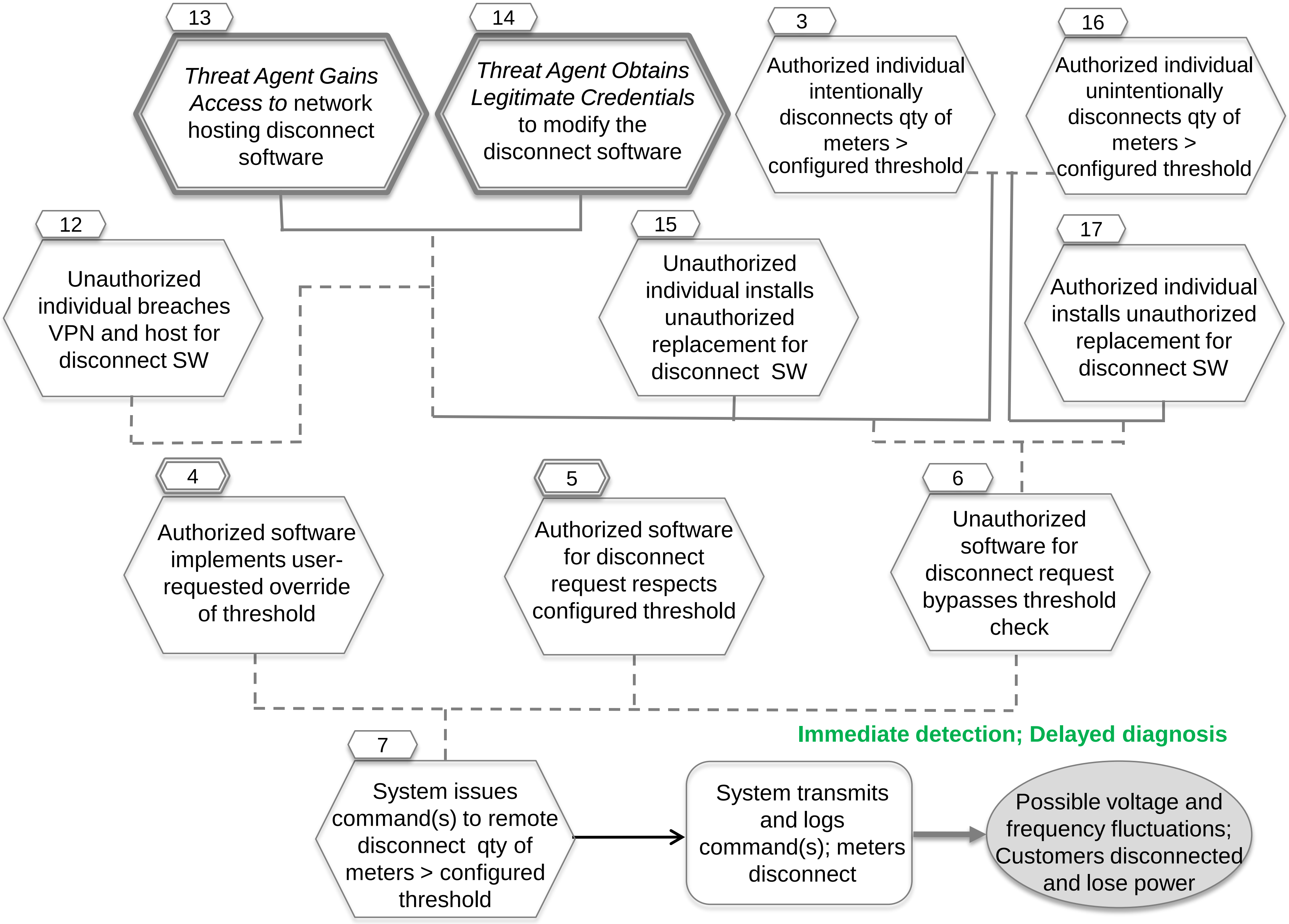
Immediate detection; Delayed diagnosis

7 System issues command(s) to remote disconnect qty of meters > configured threshold

System transmits and logs command(s); meters disconnect

Possible voltage and frequency fluctuations; Customers disconnected and lose power

AMI.1 Authorized Individual Issues Unauthorized Mass Remote Disconnect (3/3)



13

Threat Agent Gains Access to network hosting disconnect software

14

Threat Agent Obtains Legitimate Credentials to modify the disconnect software

3

Authorized individual intentionally disconnects qty of meters > configured threshold

16

Authorized individual unintentionally disconnects qty of meters > configured threshold

12

Unauthorized individual breaches VPN and host for disconnect SW

15

Unauthorized individual installs unauthorized replacement for disconnect SW

17

Authorized individual installs unauthorized replacement for disconnect SW

4

Authorized software implements user-requested override of threshold

5

Authorized software for disconnect request respects configured threshold

6

Unauthorized software for disconnect request bypasses threshold check

Immediate detection; Delayed diagnosis

7

System issues command(s) to remote disconnect qty of meters > configured threshold

System transmits and logs command(s); meters disconnect

Possible voltage and frequency fluctuations; Customers disconnected and lose power

AMI.1 Mass Meter Remote Disconnect by Authorized Individual

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

Potential Mitigations

1 – *Verify personnel* using background checks

2 – See common sub tree *Threat Agent Uses Social Engineering*

3 – *Limit events:* do not support override of number of disconnects*; require 2 person rule* for override

6 - *Require application whitelisting*

8 – See common sub tree *Threat Agent Gains Access to <network >*

9 – See common sub tree *Threat Agent Obtains Legitimate Credentials* for <system or function>

10 ,11 – *Require 2 person rule*; *generate alert* for change to threshold setting or file

12 – *Create policy* for changing passwords, *maintain patches* in VPN SW

12 – *require strong host password* or other credentials; *harden platform* of host

13 – See common sub tree *Threat Agent Gains Access to <network >*

AMI.1 Mass Meter Remote Disconnect by Authorized Individual

Potential Mitigations (2)

14 – See common sub tree *Threat Agent Obtains Legitimate Credentials* for <system or function>

15 – *check SW file integrity*

16 – none

15, 17 – *generate alert* on changes to critical files

AMI.9 Invalid Disconnect Messages to Meters Impact Customers and Utility

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

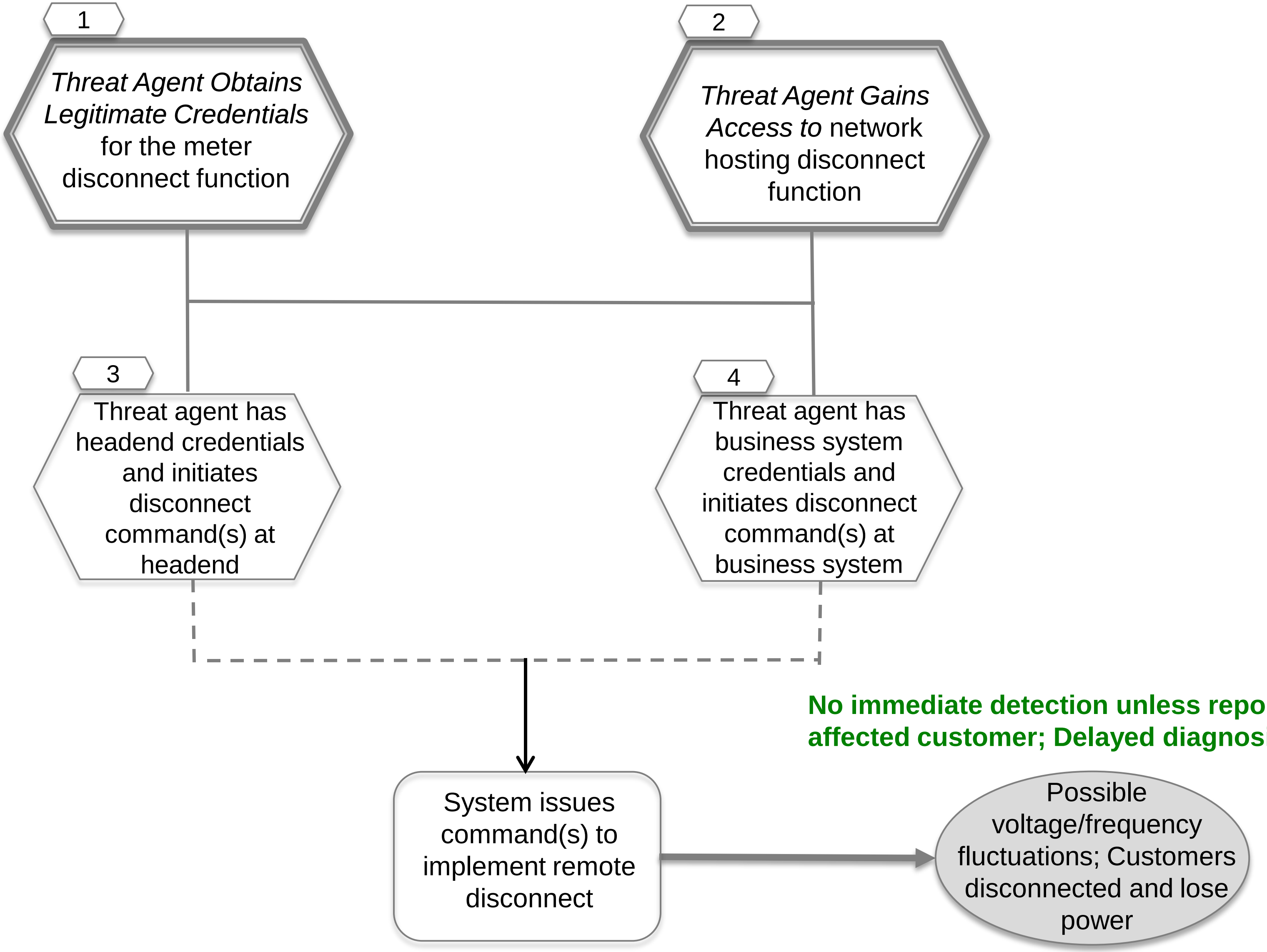
Description

A threat agent obtains legitimate credentials to the AMI system via social engineering. The threat agent may already have access to the network on which this system resides or may succeed in reaching the network from another network. The threat agent issues a disconnect command for one or more target meters. Alternatively, a disconnect may be placed in a schedule and then occur automatically at a later time.

Assumptions

- No Internet access from AMI headend
- A limited number of individuals have privilege to do disconnects

AMI.9: Unauthorized Disconnect Messages to Meters



1

Threat Agent Obtains Legitimate Credentials for the meter disconnect function

2

Threat Agent Gains Access to network hosting disconnect function

3

Threat agent has headend credentials and initiates disconnect command(s) at headend

4

Threat agent has business system credentials and initiates disconnect command(s) at business system

System issues command(s) to implement remote disconnect

Possible voltage/frequency fluctuations; Customers disconnected and lose power

No immediate detection unless reported by affected customer; Delayed diagnosis

AMI.9: Unauthorized Disconnect Messages to Meters

Potential Mitigations

1 - *Verify personnel* using background checks

1 - See common sub tree *Threat Agent Obtains Legitimate Credentials* for <system or function>

2 - See common sub tree *Threat Agent Gains Access to <Network >*

3 - *Design for security* by not permitting disconnects originating from headend (For example, require meter to verify signature by business system)

4 - *Cross check* payment status and critical service against business rules

4 - *Enforce least privilege* to a minimum number of individuals requiring MDMS access

4 - *Generate alerts* for users to another instance of their account in use (if they are logged in), and time of last login

4 - *Detect unusual patterns* of disconnects on smart meters

AMI.12: Improper Firewall Configuration Exposes Customer Data

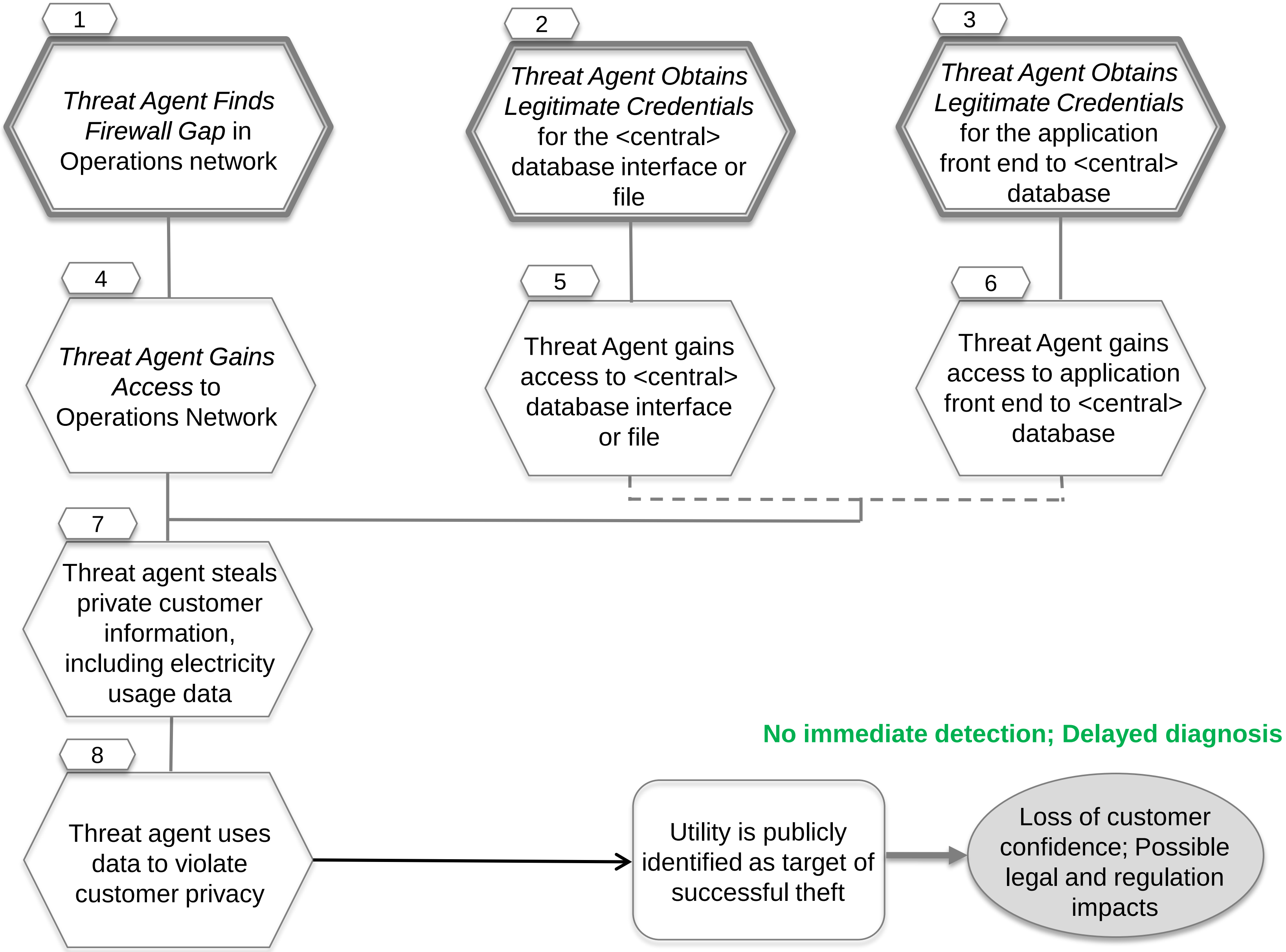
Description

A firewall rule is intentionally or unintentionally created allowing direct access from another network. Taking advantage of this rule, a threat agent subsequently gains access to the [central] database that receives data from the customer accounts database, [and from the energy usage application]. This enables the threat agent to steal customer identifiable information, including electricity usage data.

Assumptions

- Authentication and roles in place for access to customer data
- Operations network hosts customer private data

AMI.12: Improper Firewall Configuration Exposes Customer Data


1
Threat Agent Finds Firewall Gap in Operations network
2
Threat Agent Obtains Legitimate Credentials for the <central> database interface or file
3
Threat Agent Obtains Legitimate Credentials for the application front end to <central> database
4
Threat Agent Gains Access to Operations Network
5
Threat Agent gains access to <central> database interface or file
6
Threat Agent gains access to application front end to <central> database
7
Threat agent steals private customer information, including electricity usage data
8
Threat agent uses data to violate customer privacy
No immediate detection; Delayed diagnosis
Utility is publicly identified as target of successful theft
Loss of customer confidence; Possible legal and regulation impacts

AMI.12: Improper Firewall Configuration Exposes Customer Data

Potential Mitigations

- 1 – See common sub tree *Threat Agent Finds Firewall Gap*
- 2, 3 – See common sub tree *Threat Agent Obtains Legitimate Credentials*
- 4 – *Require authentication* to the network
- 4 – *Enforce least privilege* for individuals with access to hosts on the network
- 4 – *Detect unusual patterns* of usage on hosts and network
- *5, 6 - Enforce least privilege* to limit central database/application access to authorized applications and/or locally authenticated users

AMI.14 Breach of Cellular Provider's Network Exposes AMI Access

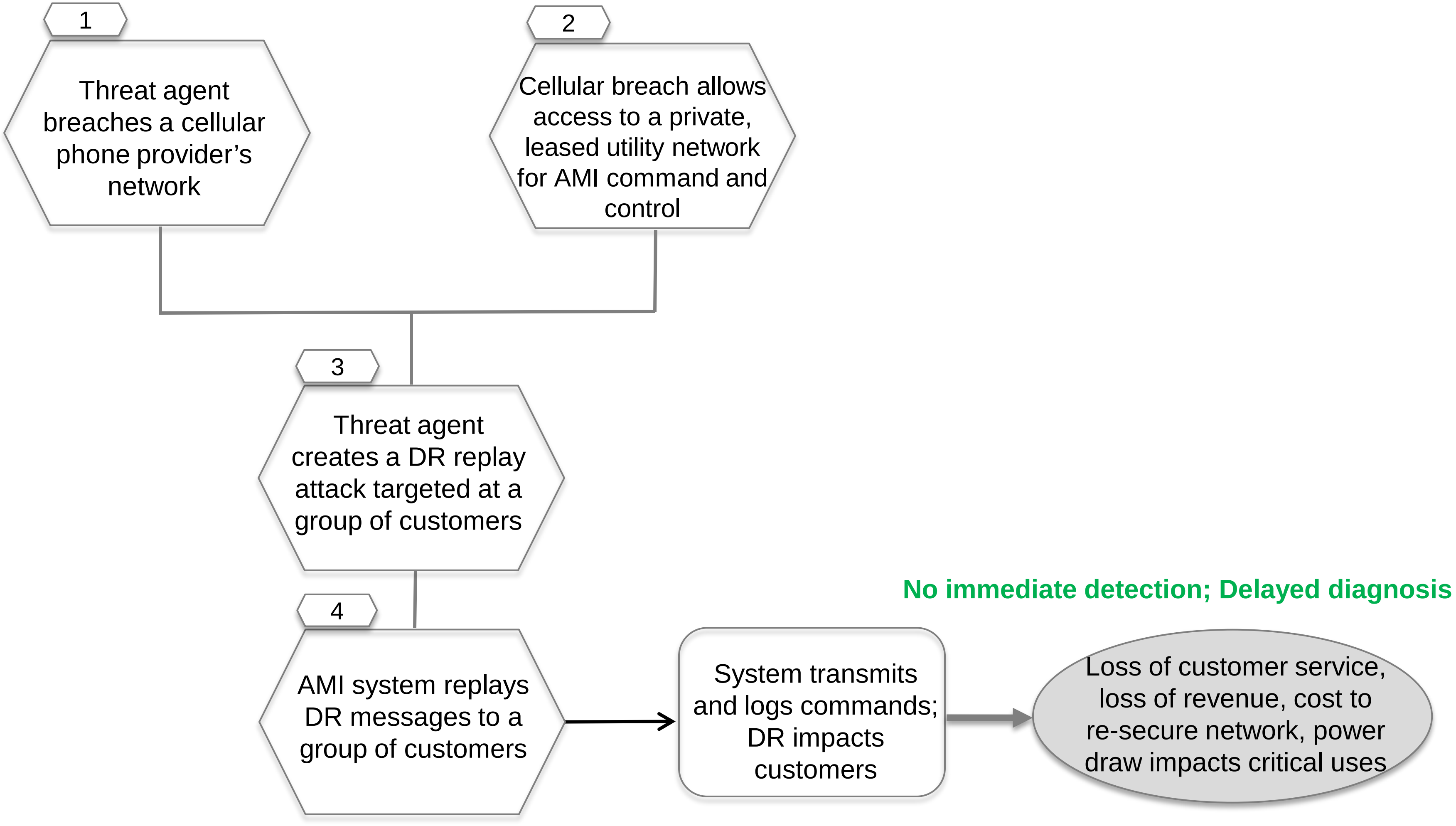
Description

A cellular phone provider's network is breached, allowing access to a private network leased to a utility for AMI command and control. The AMI implementation is vulnerable to replay attacks and DR messages are replayed to a group of customers.

Assumptions

- Inadequate separation of private leased networks between cellular phone provider and leased utility network for AMI
- Weak or no cryptography for network access
- Replay ability for commands

AMI.14: Breach of Cellular Provider's Network Exposes AMI Access



1

Threat agent breaches a cellular phone provider's network

2

Cellular breach allows access to a private, leased utility network for AMI command and control

3

Threat agent creates a DR replay attack targeted at a group of customers

4

AMI system replays DR messages to a group of customers

System transmits and logs commands; DR impacts customers

No immediate detection; Delayed diagnosis

Loss of customer service, loss of revenue, cost to re-secure network, power draw impacts critical uses

AMI.14 Breach of Cellular Provider's Network Exposes AMI Access

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

Potential Mitigations

1, 2 - *Isolate networks* using different encryption keys to prevent a breach in one network from affecting another network

2 - Require approved cryptographic algorithms at the link layer to prevent a threat agent from being able to affect the confidentiality and integrity on the AMI network if a breach should occur

3 - Protect against replay using time-stamping or other methods

AMI.16: Compromised Headend Allows Impersonation of CA

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

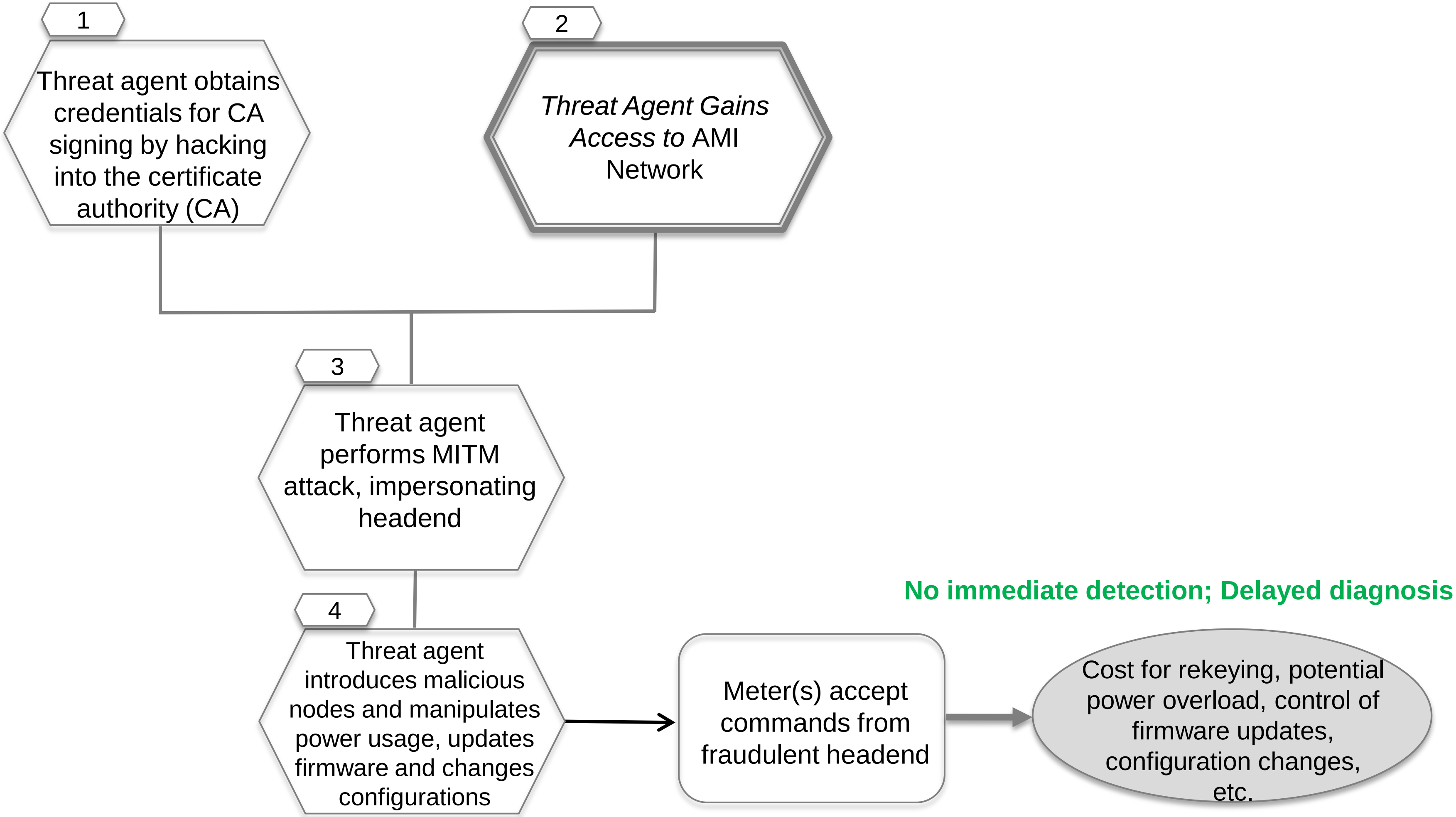
Description

The private key for the certificate authority (CA) used to set up a Public Key Infrastructure (PKI) at the head end is compromised, which allows a threat agent to impersonate the CA.

Assumptions

- No cryptography for AMI network access
- PKI is used on the AMI network

AMI.16: Compromised Headend Allows Impersonation of CA


1
Threat agent obtains credentials for CA signing by hacking into the certificate authority (CA)
2
Threat Agent Gains Access to AMI Network
3
Threat agent performs MITM attack, impersonating headend
4
Threat agent introduces malicious nodes and manipulates power usage, updates firmware and changes configurations
Meter(s) accept commands from fraudulent headend
No immediate detection; Delayed diagnosis
Cost for rekeying, potential power overload, control of firmware updates, configuration changes, etc.

AMI.16: Compromised Headend Allows Impersonation of CA

Research conducted by EPRI for:
NESCOR – a DOE funded
public-private partnership

Potential Mitigations

1 – *Require approved key management* including secure generation, distribution, storage, and update of cryptographic keys

2 – See common sub tree *Threat Agent Gains Access to* <network>

AMI.27: Reverse Engineering of AMI Equipment Allows Unauthorized Mass Control

Research conducted by EPRI for:
NESCOR – a DOE funded
public-private partnership

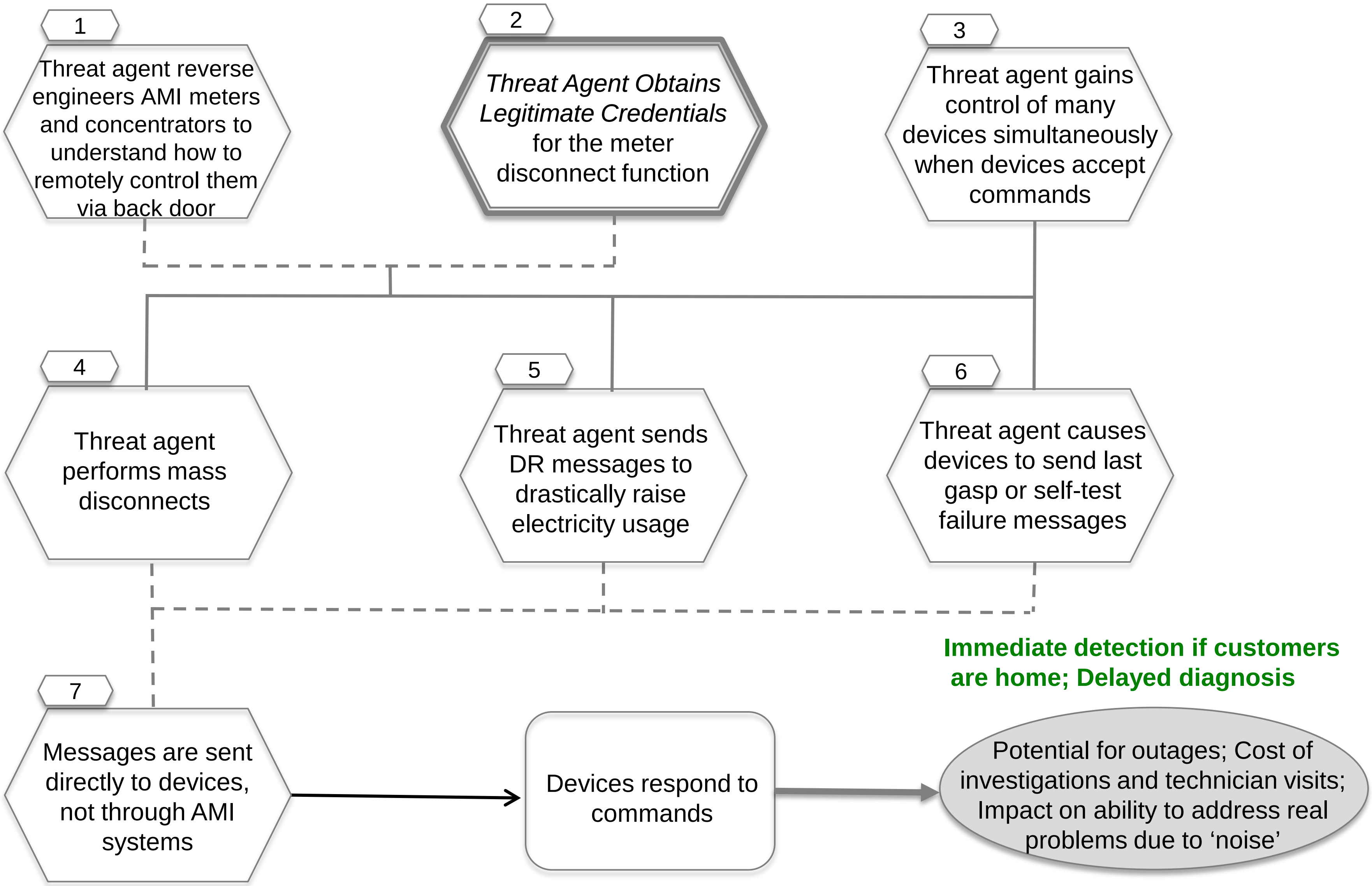
Description

A threat agent is able to reverse engineer AMI equipment (meters and concentrators) to determine how to remotely control them. This allows the threat agent to control many devices simultaneously, and, for example, to perform a simultaneous mass disconnect, send DR messages that cause consumption of electricity to go up dramatically, or cause devices to send out last gasp or self-test failed messages.

Assumptions

- Devices are not built with adequate security
- Backdoors and unprotected interfaces remain on production equipment

AMI.27: Reverse Engineering of AMI Equipment Allows Unauthorized Mass Control



1 Threat agent reverse engineers AMI meters and concentrators to understand how to remotely control them via back door

2 *Threat Agent Obtains Legitimate Credentials* for the meter disconnect function

3 Threat agent gains control of many devices simultaneously when devices accept commands

4 Threat agent performs mass disconnects

5 Threat agent sends DR messages to drastically raise electricity usage

6 Threat agent causes devices to send last gasp or self-test failure messages

7 Messages are sent directly to devices, not through AMI systems

Devices respond to commands

Immediate detection if customers are home; Delayed diagnosis

Potential for outages; Cost of investigations and technician visits; Impact on ability to address real problems due to ‘noise’

AMI.27: Reverse Engineering of AMI Equipment Allows Unauthorized Mass Control

Potential Mitigations

1 – *Design for security* to identify and remove unsecure development features and nonstandard" interfaces from production devices

2 – See common tree *Threat Agent Obtains Legitimate Credentials*

3 - Design for security in equipment such that knowledge alone should not allow a threat agent to access a device without knowledge of keys and other credentials in equipment design

3 - Configure for least functionality
by removing unnecessary interfaces and labeling from production devices

AMI.29: Unauthorized Device Accesses HAN and Steals Private Information

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

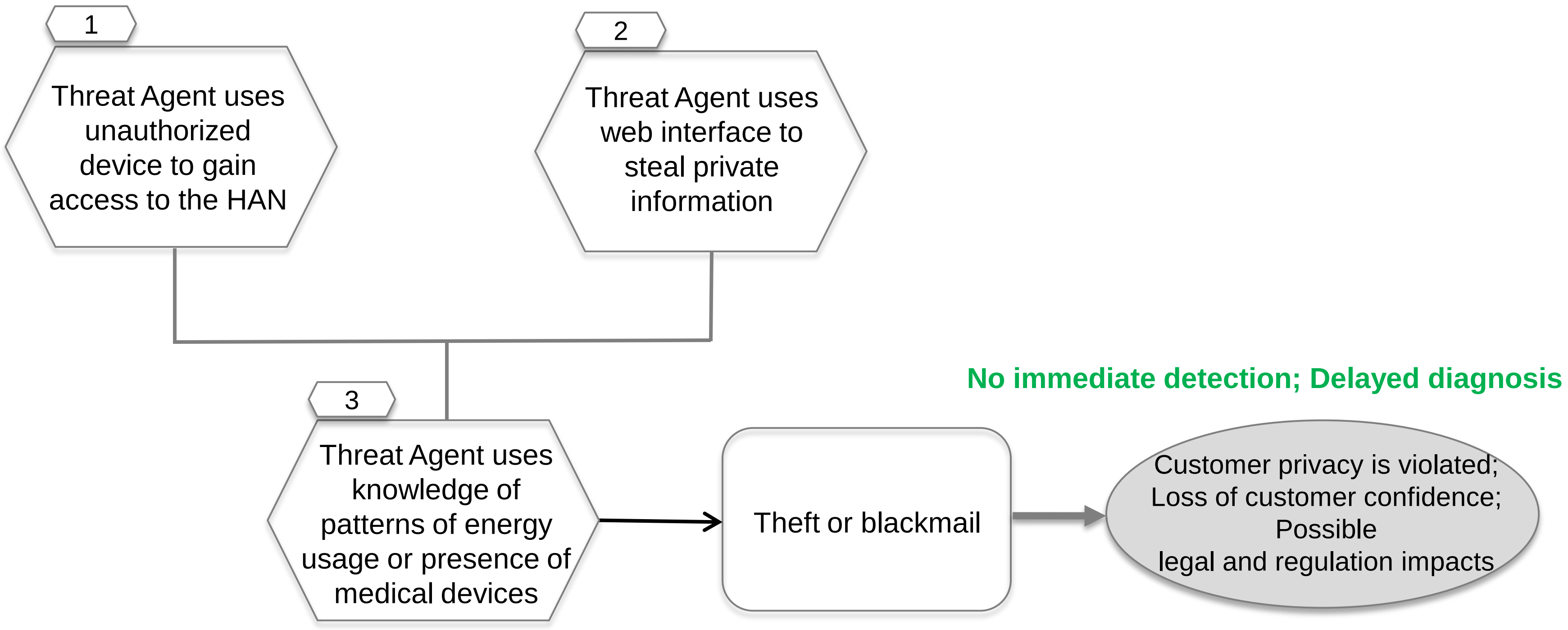
Description

An unauthorized device gains access to the HAN and uses the web interface to obtain private information. Examples of such information are patterns of energy usage and the presence of medical devices.

Assumptions

- Weak or no authentication required for HAN access

AMI.29: Unauthorized Device Acquires HAN Access and Steals Private Information



1

Threat Agent uses unauthorized device to gain access to the HAN

2

Threat Agent uses web interface to steal private information

3

Threat Agent uses knowledge of patterns of energy usage or presence of medical devices

Theft or blackmail

No immediate detection; Delayed diagnosis

Customer privacy is violated;
Loss of customer confidence;
Possible
legal and regulation impacts

AMI.29: Unauthorized Device Accesses HAN and Steals Private Information

Potential Mitigations

1 - Restrict network access to the HAN

2 - Minimize private information in HAN systems and devices

AMI.32:Power Stolen by Reconfiguring Meter via Optical Port

Research conducted by EPRI for:
NESCOR – a DOE funded
public-private partnership

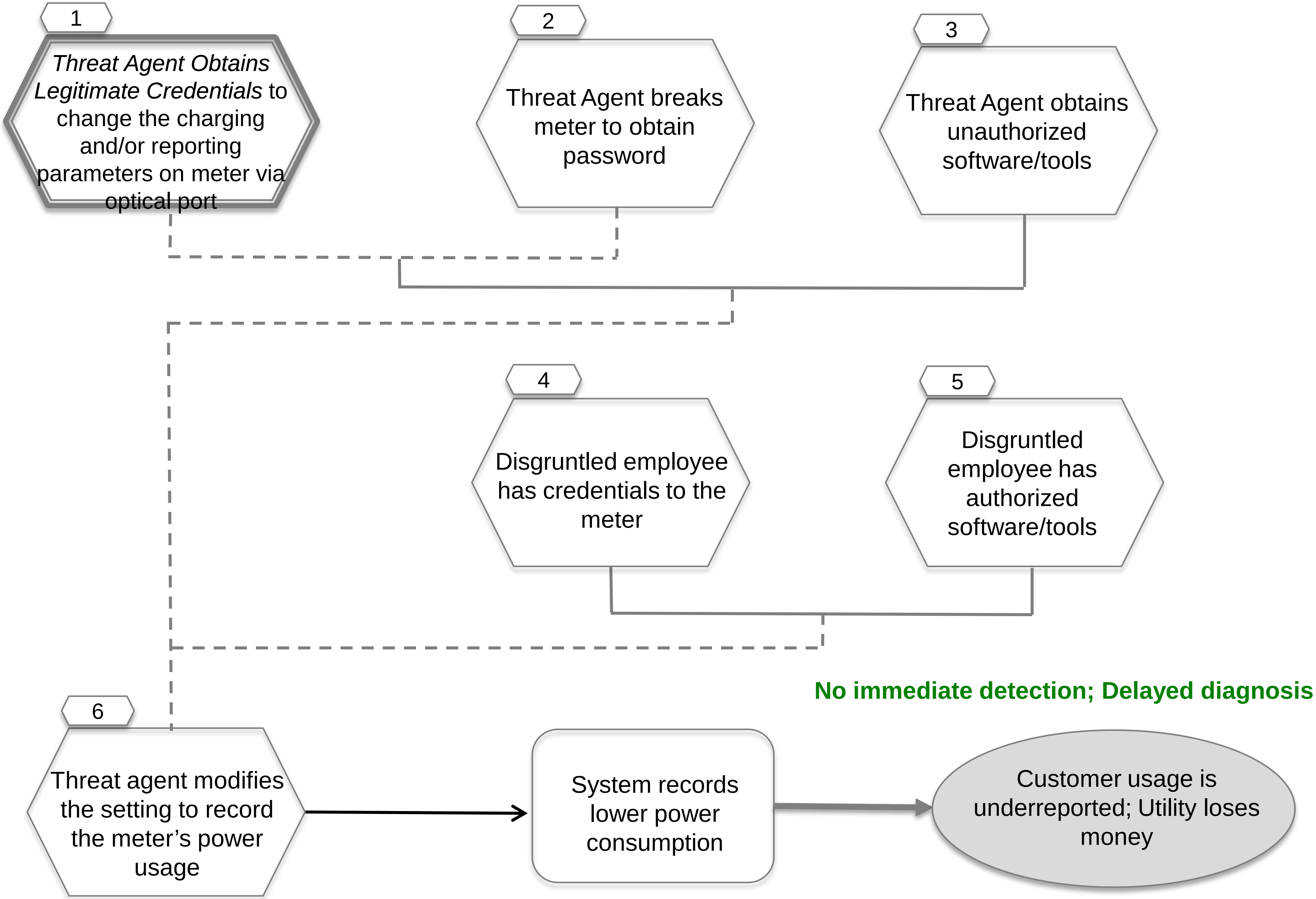
Description

Many smart meters provide the capability of re-calibrating the settings via an optical port, which is then misused by economic thieves who offer to alter the meters for a fee, changing the settings for recording power consumption and often cutting utility bills by 50-75%. This requires collusion between a knowledgeable criminal and an electric customer, and will spread because of the ease of intrusion and the economic benefit to both parties.

Assumptions

- Weak or no authentication required for HAN access
- Meters have an optical port, and a re-configuration function accessible from the optical port
- Both insiders and outsiders have a strong motivation in financial gain
- There is sufficient information and tools available to teach outsiders how to do this attack
- Threat agent has physical access to meter

AMI.32: Power Stolen by Reconfiguring Meter via Optical Port


1
Threat Agent Obtains Legitimate Credentials to change the charging and/or reporting parameters on meter via optical port
2
Threat Agent breaks meter to obtain password
3
Threat Agent obtains unauthorized software/tools
4
Disgruntled employee has credentials to the meter
5
Disgruntled employee has authorized software/tools
6
Threat agent modifies the setting to record the meter's power usage
System records lower power consumption
Customer usage is underreported; Utility loses money

No immediate detection; Delayed diagnosis

AMI.32: Power Stolen by Reconfiguring Meter via Optical Port

Potential Mitigations

1 - See common sub tree *Threat Agent Obtains Legitimate Credentials*

2, 4, 5 - Require multi-factor authentication for firmware updates

6 - Detect unusual patterns of energy usage on smart meters (all utilities have some type of revenue protection scheme, but these may not be sufficient)

6 - Check software file integrity (digital signatures) on code files to validate firmware updates before installation

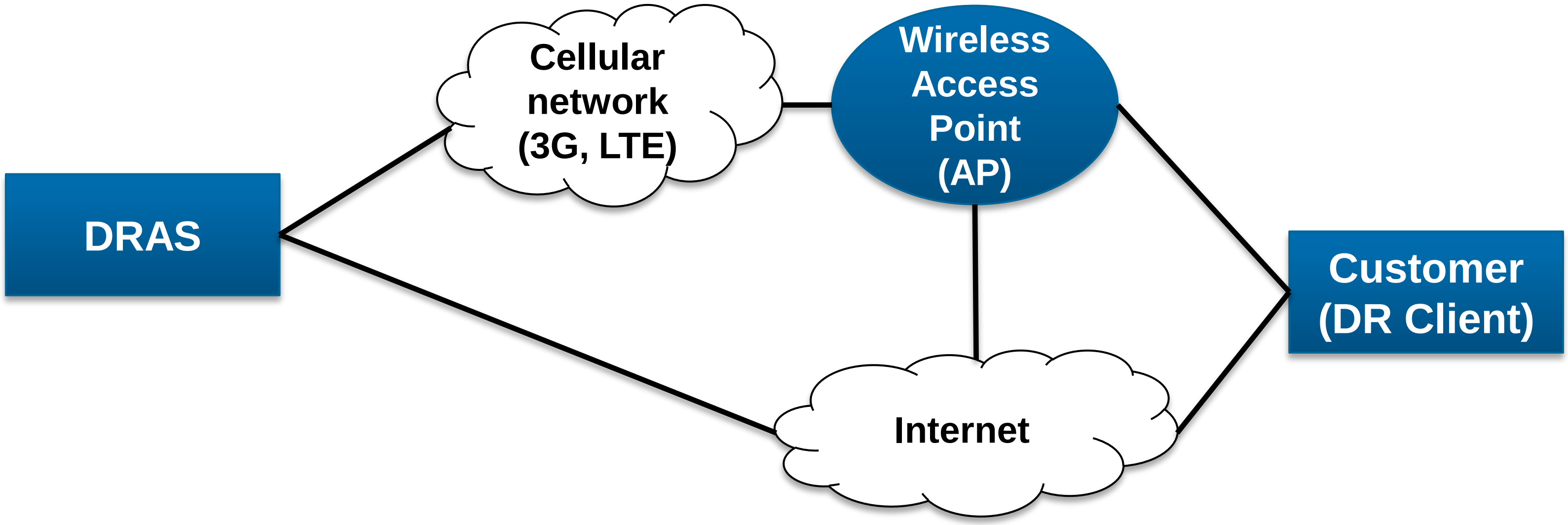
DR.1 Blocked DR Messages Result in Increased Prices or Outages

Description

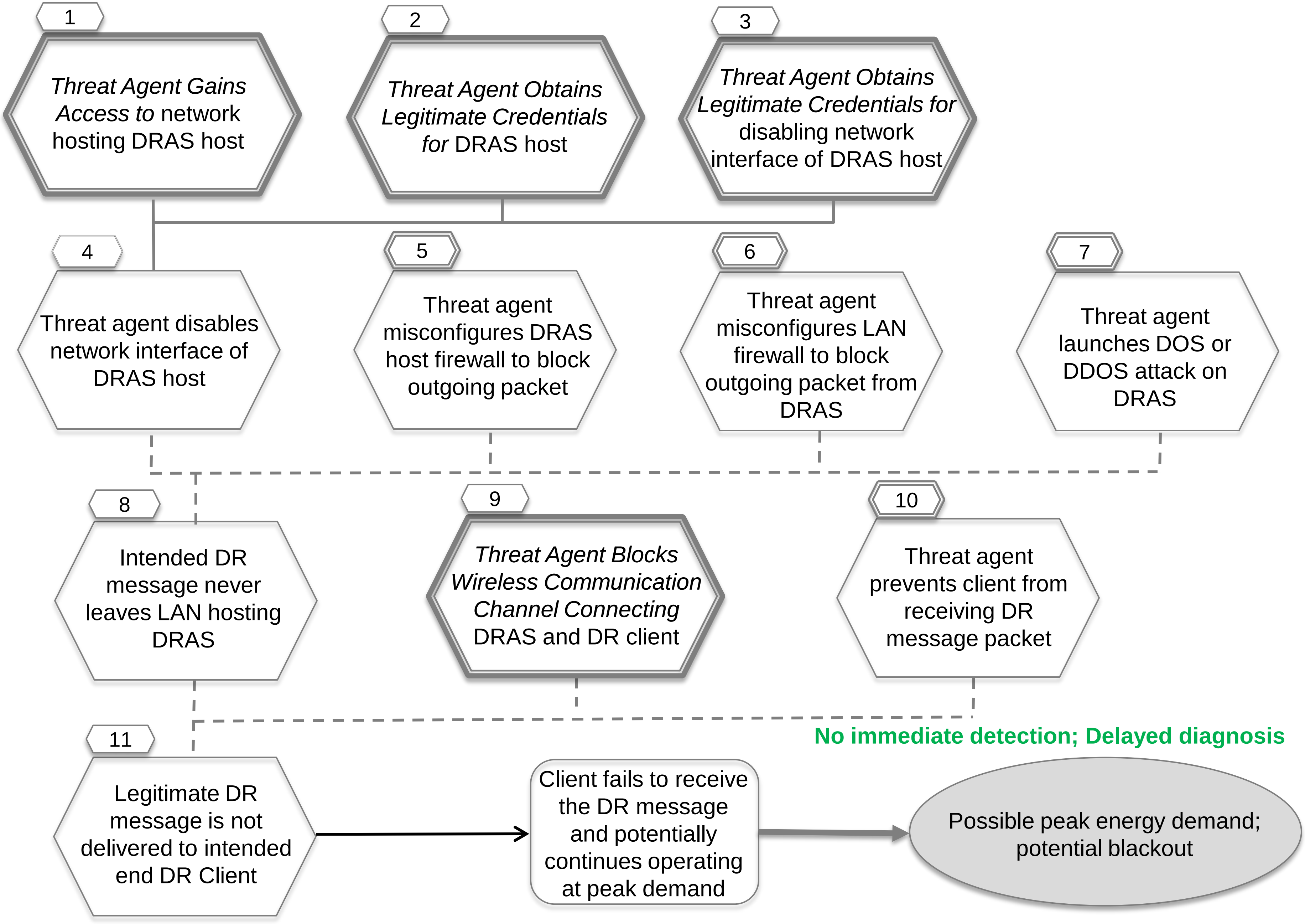
A threat agent blocks communications between a demand response automation server (DRAS) and a customer system (smart meters or customer devices). This could be accomplished by flooding the communications channel with other messages, or by tampering with the communications channel. These actions could prevent legitimate DR messages from being received and transmitted. This can occur at the wired or the wireless portion of the communications channel.

DR.1 Blocked DR Messages Result in Increased Prices or Outages

Related Architecture



DR.1 Blocked DR Messages Result in Increased Prices or Outages (1/8)



1 *Threat Agent Gains Access to* network hosting DRAS host

2 *Threat Agent Obtains Legitimate Credentials for* DRAS host

3 *Threat Agent Obtains Legitimate Credentials for* disabling network interface of DRAS host

4 Threat agent disables network interface of DRAS host

5 Threat agent misconfigures DRAS host firewall to block outgoing packet

6 Threat agent misconfigures LAN firewall to block outgoing packet from DRAS

7 Threat agent launches DOS or DDOS attack on DRAS

8 Intended DR message never leaves LAN hosting DRAS

9 *Threat Agent Blocks Wireless Communication Channel Connecting* DRAS and DR client

10 Threat agent prevents client from receiving DR message packet

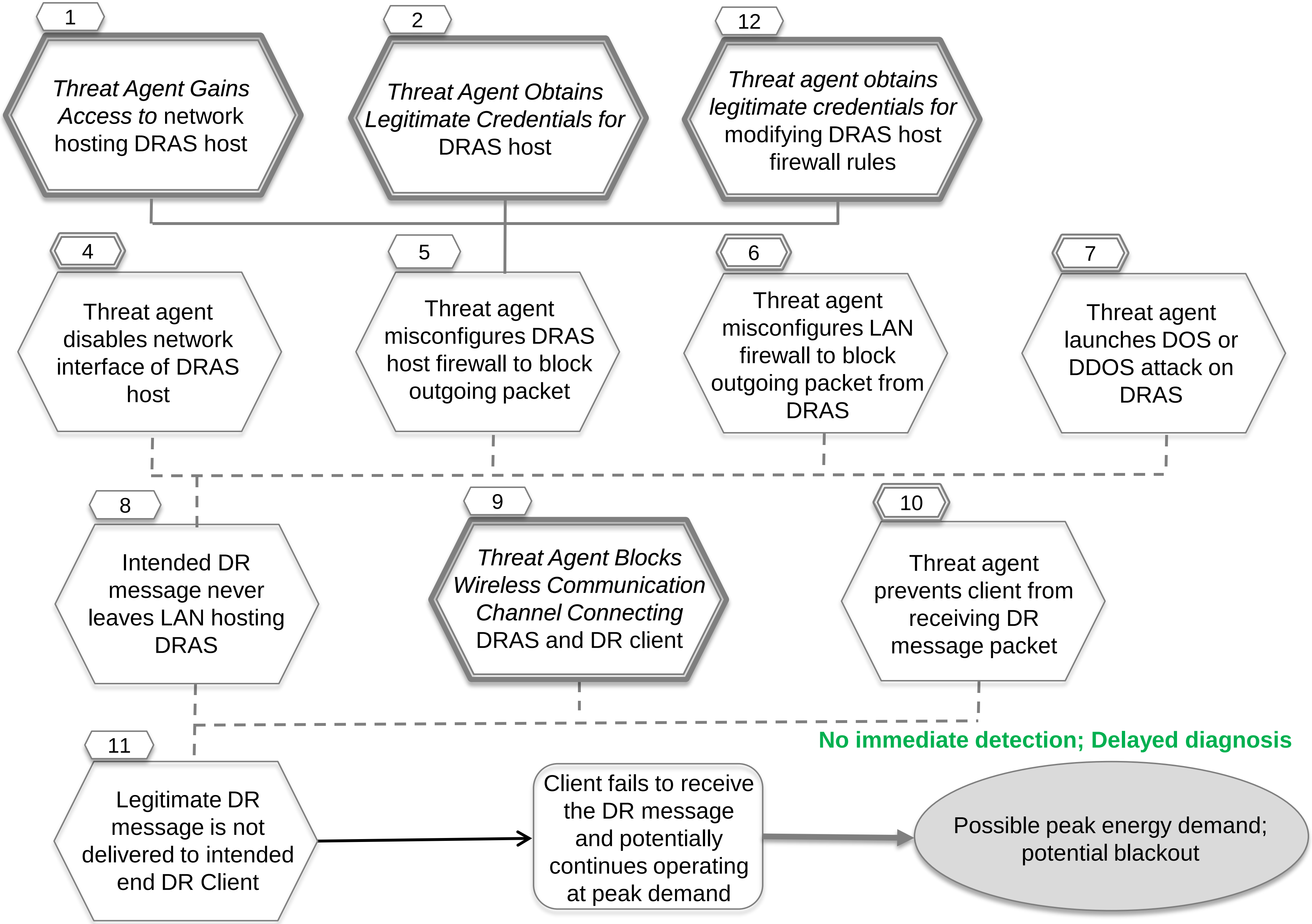
11 Legitimate DR message is not delivered to intended end DR Client

Client fails to receive the DR message and potentially continues operating at peak demand

No immediate detection; Delayed diagnosis

Possible peak energy demand; potential blackout

DR.1 Blocked DR Messages Result in Increased Prices or Outages (2/8)



1 *Threat Agent Gains Access to* network hosting DRAS host

2 *Threat Agent Obtains Legitimate Credentials for* DRAS host

12 *Threat agent obtains legitimate credentials for* modifying DRAS host firewall rules

4 Threat agent disables network interface of DRAS host

5 Threat agent misconfigures DRAS host firewall to block outgoing packet

6 Threat agent misconfigures LAN firewall to block outgoing packet from DRAS

7 Threat agent launches DOS or DDOS attack on DRAS

8 Intended DR message never leaves LAN hosting DRAS

9 *Threat Agent Blocks Wireless Communication Channel Connecting* DRAS and DR client

10 Threat agent prevents client from receiving DR message packet

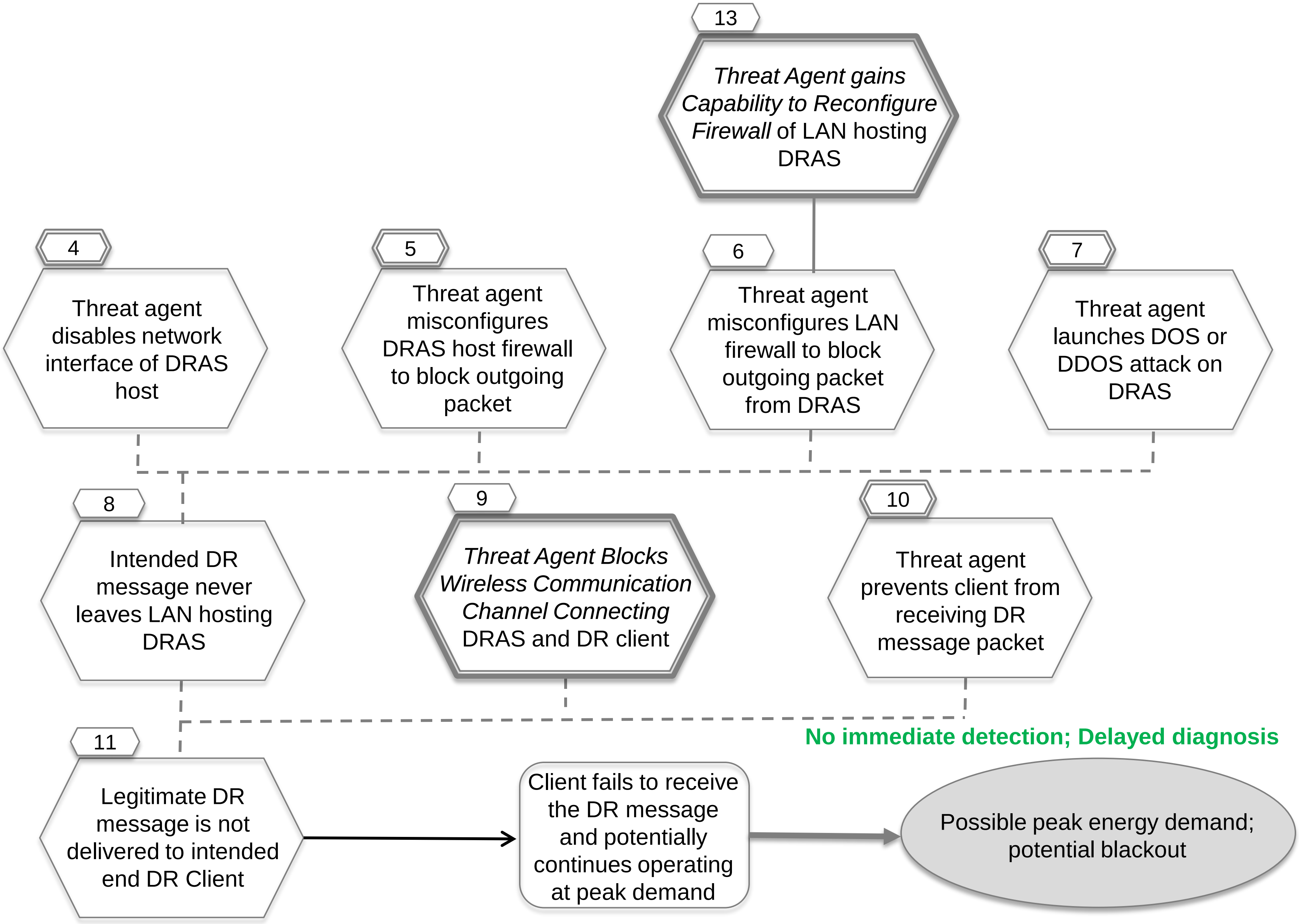
No immediate detection; Delayed diagnosis

11 Legitimate DR message is not delivered to intended end DR Client

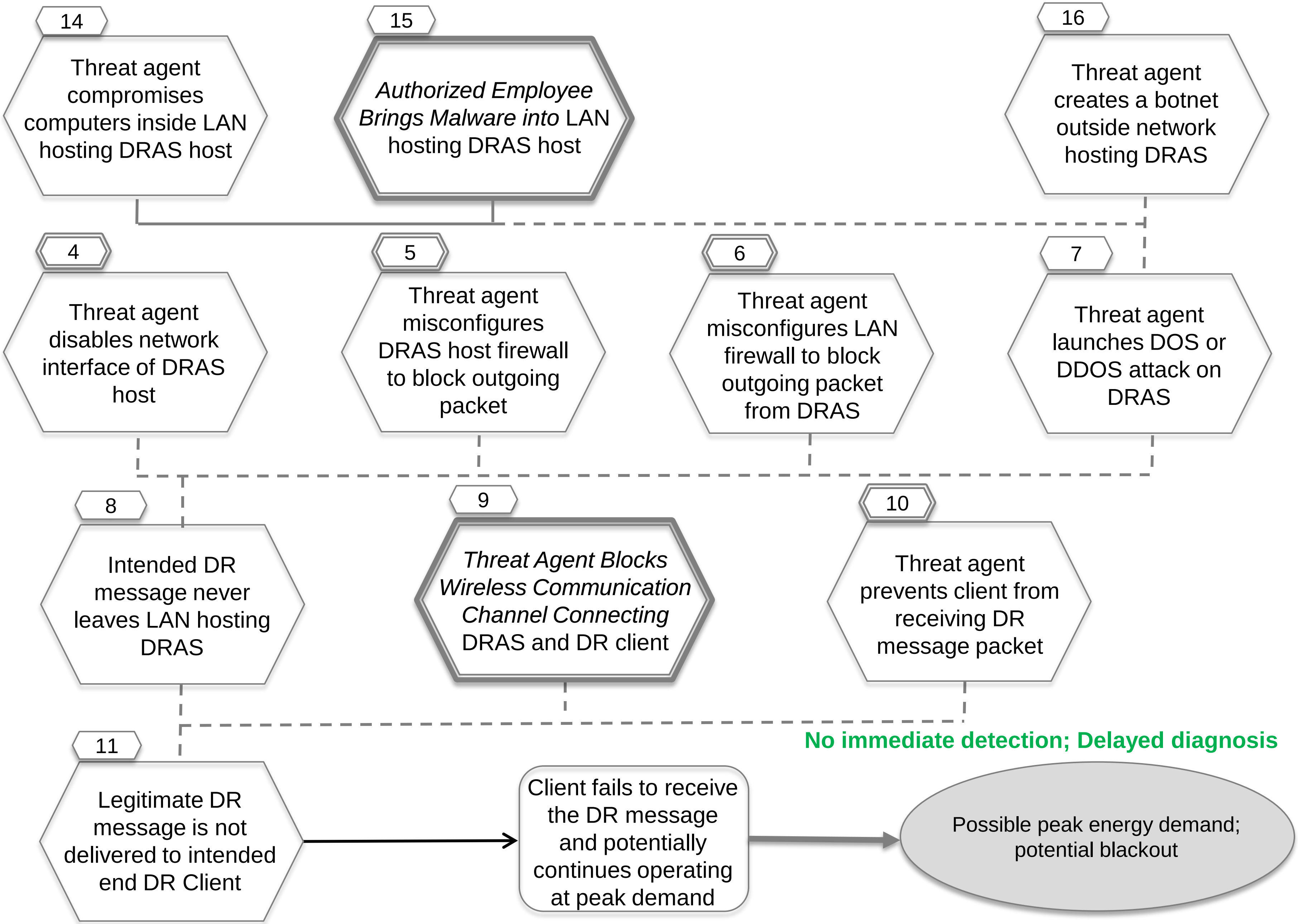
Client fails to receive the DR message and potentially continues operating at peak demand

Possible peak energy demand; potential blackout

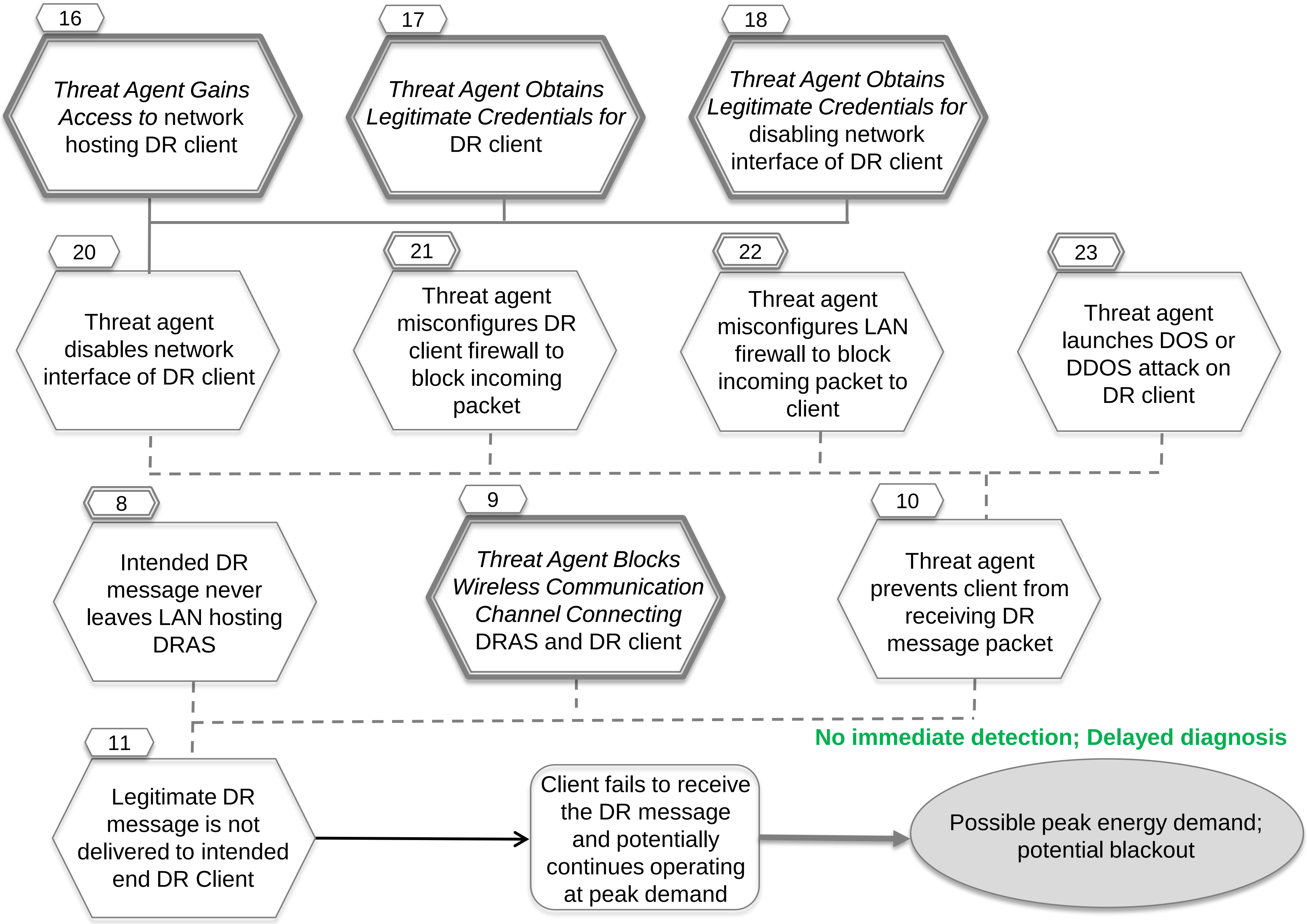
DR.1 Blocked DR Messages Result in Increased Prices or Outages (3/8)


13
Threat Agent gains Capability to Reconfigure Firewall of LAN hosting DRAS
4
Threat agent disables network interface of DRAS host
5
Threat agent misconfigures DRAS host firewall to block outgoing packet
6
Threat agent misconfigures LAN firewall to block outgoing packet from DRAS
7
Threat agent launches DOS or DDOS attack on DRAS
8
Intended DR message never leaves LAN hosting DRAS
9
Threat Agent Blocks Wireless Communication Channel Connecting DRAS and DR client
10
Threat agent prevents client from receiving DR message packet
No immediate detection; Delayed diagnosis
11
Legitimate DR message is not delivered to intended end DR Client
Client fails to receive the DR message and potentially continues operating at peak demand
Possible peak energy demand; potential blackout

DR.1 Blocked DR Messages Result in Increased Prices or Outages (4/8)


14
Threat agent compromises computers inside LAN hosting DRAS host
15
Authorized Employee Brings Malware into LAN hosting DRAS host
16
Threat agent creates a botnet outside network hosting DRAS
4
Threat agent disables network interface of DRAS host
5
Threat agent misconfigures DRAS host firewall to block outgoing packet
6
Threat agent misconfigures LAN firewall to block outgoing packet from DRAS
7
Threat agent launches DOS or DDOS attack on DRAS
8
Intended DR message never leaves LAN hosting DRAS
9
Threat Agent Blocks Wireless Communication Channel Connecting DRAS and DR client
10
Threat agent prevents client from receiving DR message packet
No immediate detection; Delayed diagnosis
11
Legitimate DR message is not delivered to intended end DR Client
Client fails to receive the DR message and potentially continues operating at peak demand
Possible peak energy demand; potential blackout

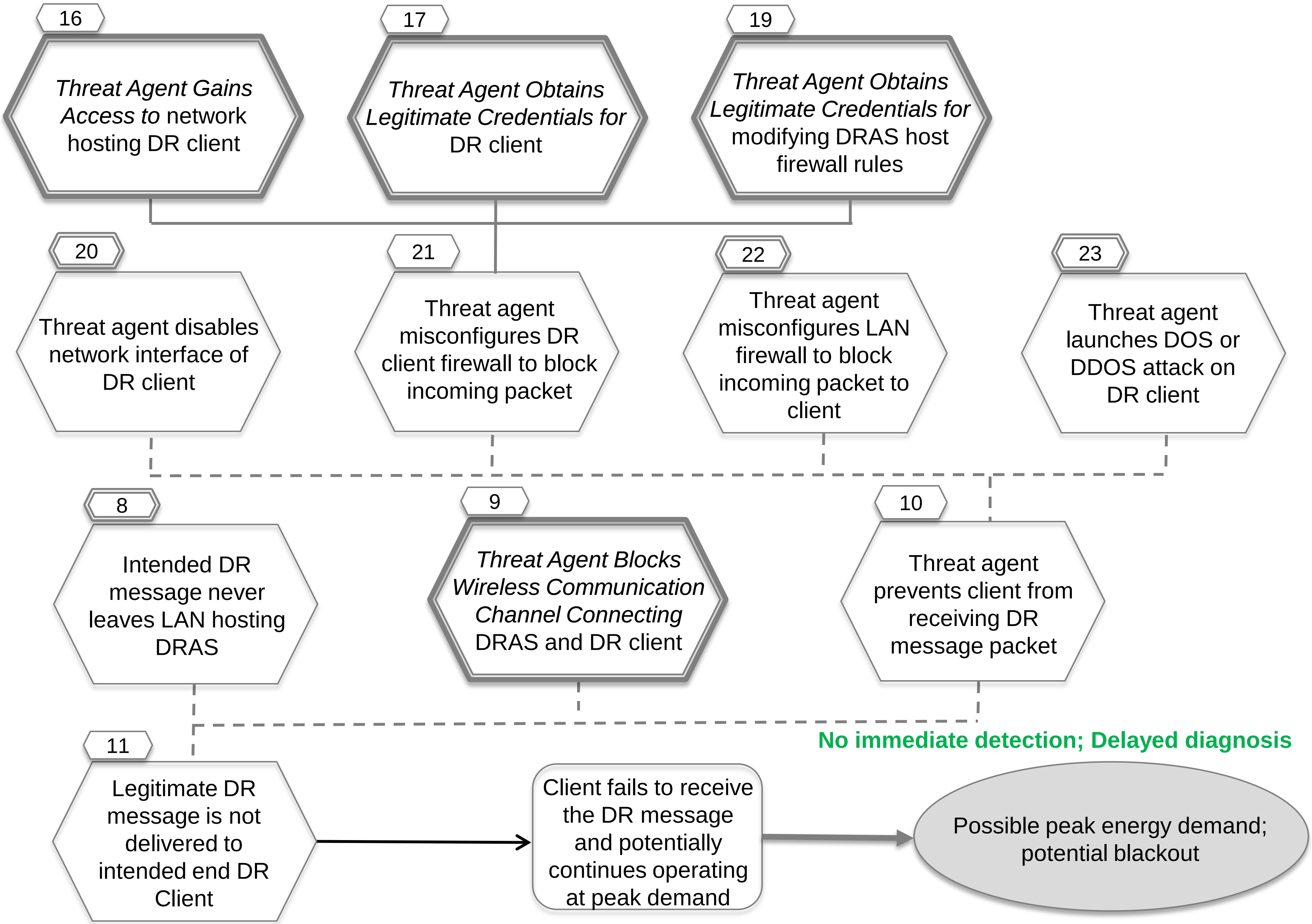
DR.1 Blocked DR Messages Result in Increased Prices or Outages (5/8)



16
Threat Agent Gains Access to network hosting DR client
17
Threat Agent Obtains Legitimate Credentials for DR client
18
Threat Agent Obtains Legitimate Credentials for disabling network interface of DR client
20
Threat agent disables network interface of DR client
21
Threat agent misconfigures DR client firewall to block incoming packet
22
Threat agent misconfigures LAN firewall to block incoming packet to client
23
Threat agent launches DOS or DDOS attack on DR client
8
Intended DR message never leaves LAN hosting DRAS
9
Threat Agent Blocks Wireless Communication Channel Connecting DRAS and DR client
10
Threat agent prevents client from receiving DR message packet
11
Legitimate DR message is not delivered to intended end DR Client
Client fails to receive the DR message and potentially continues operating at peak demand
Possible peak energy demand; potential blackout

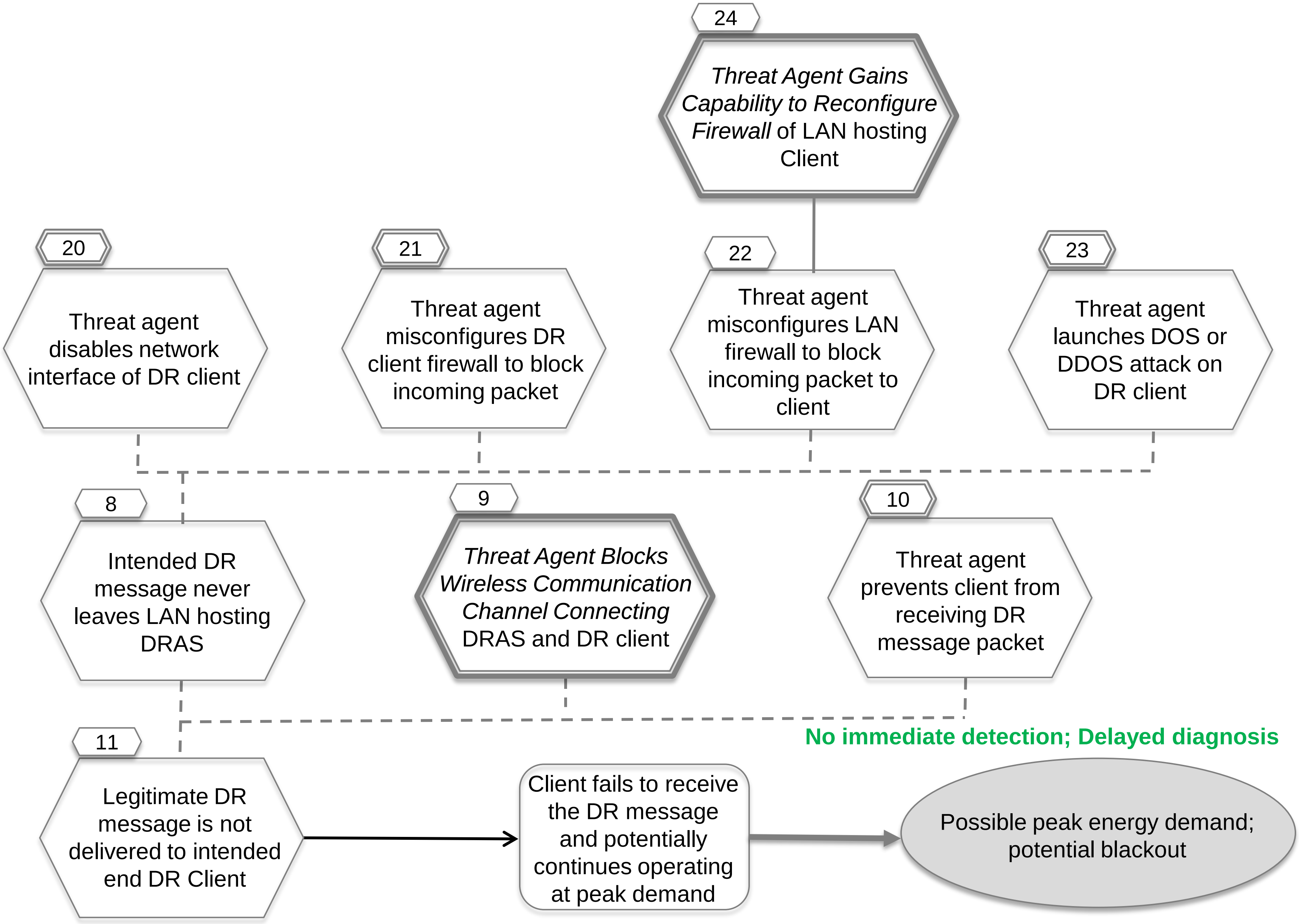
No immediate detection; Delayed diagnosis

DR.1 Blocked DR Messages Result in Increased Prices or Outages (6/8)



16
Threat Agent Gains Access to network hosting DR client
17
Threat Agent Obtains Legitimate Credentials for DR client
19
Threat Agent Obtains Legitimate Credentials for modifying DRAS host firewall rules
20
Threat agent disables network interface of DR client
21
Threat agent misconfigures DR client firewall to block incoming packet
22
Threat agent misconfigures LAN firewall to block incoming packet to client
23
Threat agent launches DOS or DDOS attack on DR client
8
Intended DR message never leaves LAN hosting DRAS
9
Threat Agent Blocks Wireless Communication Channel Connecting DRAS and DR client
10
Threat agent prevents client from receiving DR message packet
No immediate detection; Delayed diagnosis
11
Legitimate DR message is not delivered to intended end DR Client
Client fails to receive the DR message and potentially continues operating at peak demand
Possible peak energy demand; potential blackout

DR.1 Blocked DR Messages Result in Increased Prices or Outages (7/8)



24

Threat Agent Gains Capability to Reconfigure Firewall of LAN hosting Client

20

Threat agent disables network interface of DR client

21

Threat agent misconfigures DR client firewall to block incoming packet

22

Threat agent misconfigures LAN firewall to block incoming packet to client

23

Threat agent launches DOS or DDOS attack on DR client

8

Intended DR message never leaves LAN hosting DRAS

9

Threat Agent Blocks Wireless Communication Channel Connecting DRAS and DR client

10

Threat agent prevents client from receiving DR message packet

No immediate detection; Delayed diagnosis

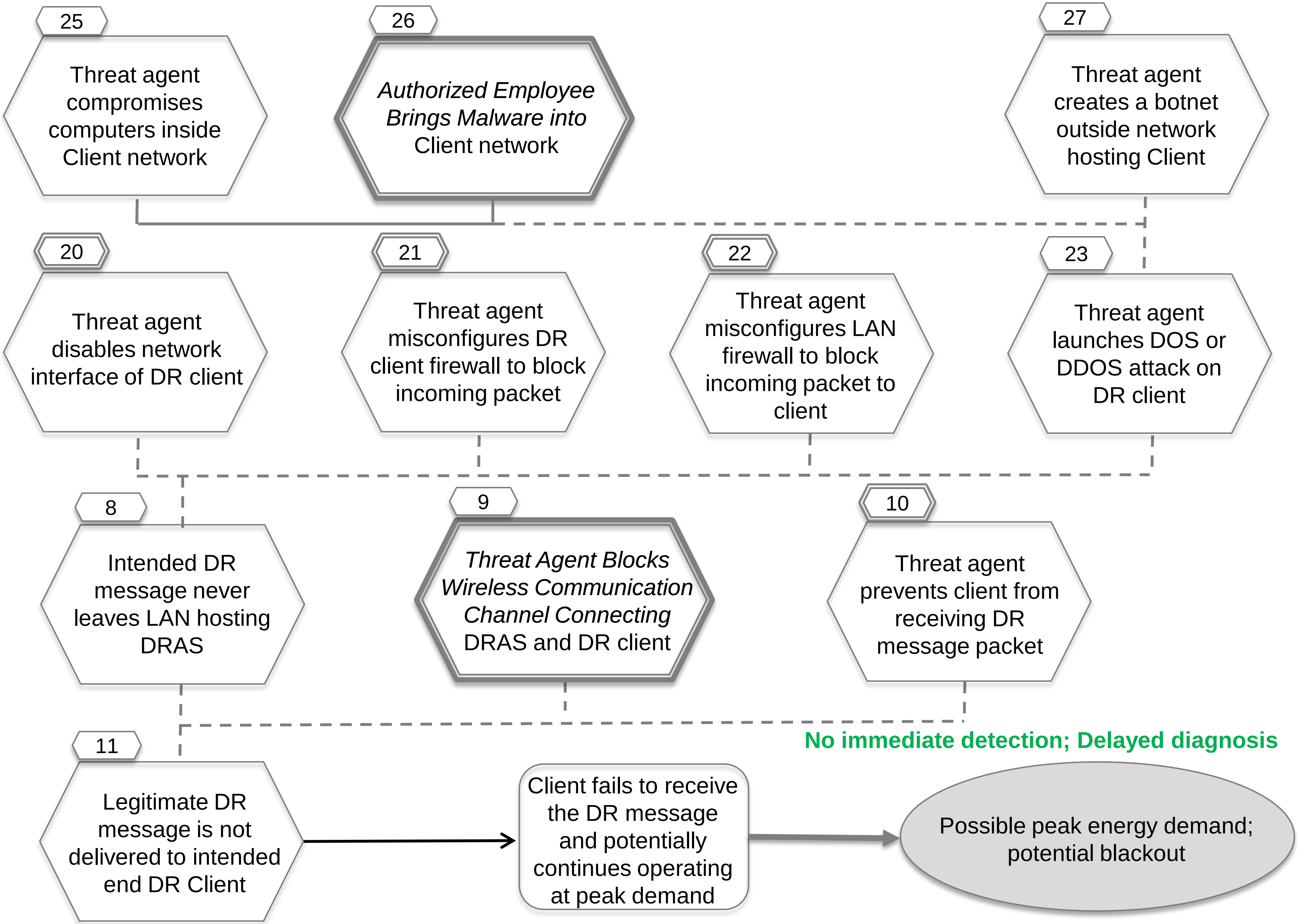
11

Legitimate DR message is not delivered to intended end DR Client

Client fails to receive the DR message and potentially continues operating at peak demand

Possible peak energy demand; potential blackout

DR.1 Blocked DR Messages Result in Increased Prices or Outages (8/8)



25
Threat agent compromises computers inside Client network
26
Authorized Employee Brings Malware into Client network
27
Threat agent creates a botnet outside network hosting Client
20
Threat agent disables network interface of DR client
21
Threat agent misconfigures DR client firewall to block incoming packet
22
Threat agent misconfigures LAN firewall to block incoming packet to client
23
Threat agent launches DOS or DDOS attack on DR client
8
Intended DR message never leaves LAN hosting DRAS
9
Threat Agent Blocks Wireless Communication Channel Connecting DRAS and DR client
10
Threat agent prevents client from receiving DR message packet
11
Legitimate DR message is not delivered to intended end DR Client
Client fails to receive the DR message and potentially continues operating at peak demand
Possible peak energy demand; potential blackout

No immediate detection; Delayed diagnosis

DR.1 Blocked DR Messages Result in Increased Prices or Outages

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

Potential Mitigations

1 - See common sub tree *Threat Agent Gains Access to <network>*

2, 3 - See common sub tree *Threat Agent Obtains Legitimate Credentials for <system or function>*

4 - *Generate alerts* on changes to device configurations on DRAS host; *Require acknowledgement* of link status to ensure network connectivity; *Detect unauthorized configuration changes*

6 - *Generate alerts* on changes to rules on LAN firewall; *Detect unauthorized changes; Create audit log* of packet filtering rule changes

7 - *Require intrusion detection and prevention*; *Detect unusual patterns* of network traffic; *Enforce restrictive firewall rules* for DRAS LAN access

9 - See common sub tree *Threat Agent Blocks Wireless Communication Channel Connecting <x and y>*

12 - See common sub tree *Threat Agent Obtains Legitimate Credentials for <system or function>*

DR.1 Blocked DR Messages Result in Increased Prices or Outages

Potential Mitigations (2)

13 - See common sub tree *Threat Agent Gains Capability to Reconfigure Firewall <firewall description>*

14 - *Maintain patches* in all computers; *Maintain anti-virus; Test for malware*; *Restrict remote access* to internal computers

15 - See common sub tree *Authorized Employee Brings Malware into <system or network>*

16 - See common sub *tree Threat Agent Gains Access to <network>*

17, 18, 19 - See common sub tree *Threat Agent Obtains Legitimate Credentials for <system or function>*

20 – *Generate alerts* on changes to device configurations on DR client; *Require acknowledgement* of link status to ensure network connectivity; *Detect unauthorized configuration changes*

21 – *Generate alerts* on changes to configurations on DR client; *Require acknowledgement* of link status to ensure network connectivity; *Detect unauthorized configuration changes*

DR.1 Blocked DR Messages Result in Increased Prices or Outages

Research conducted by EPRI for:
NESCOR – a DOE funded
public-private partnership

Potential Mitigations (3)

22 – *Generate alerts* on changes to rules on LAN firewall; *Detect unauthorized configuration changes; Create audit log* of packet filtering rule changes

23 – *Require intrusion detection and prevention*; *Detect unusual patterns* of network traffic; *Enforce restrictive firewall rules* for Client LAN access

24 – See common sub tree *Threat Agent Gains Capability to Reconfigure Firewall <firewall description>*

25 – *Maintain patches* in all computers; *Maintain anti-virus*; *Test for malware*; *Restrict remote access* to internal computers

26 – See common sub tree *Authorized Employee Brings Malware into <system or network>*

DR.4 Improper DRAS Configuration Causes Inappropriate DR Messages

Description

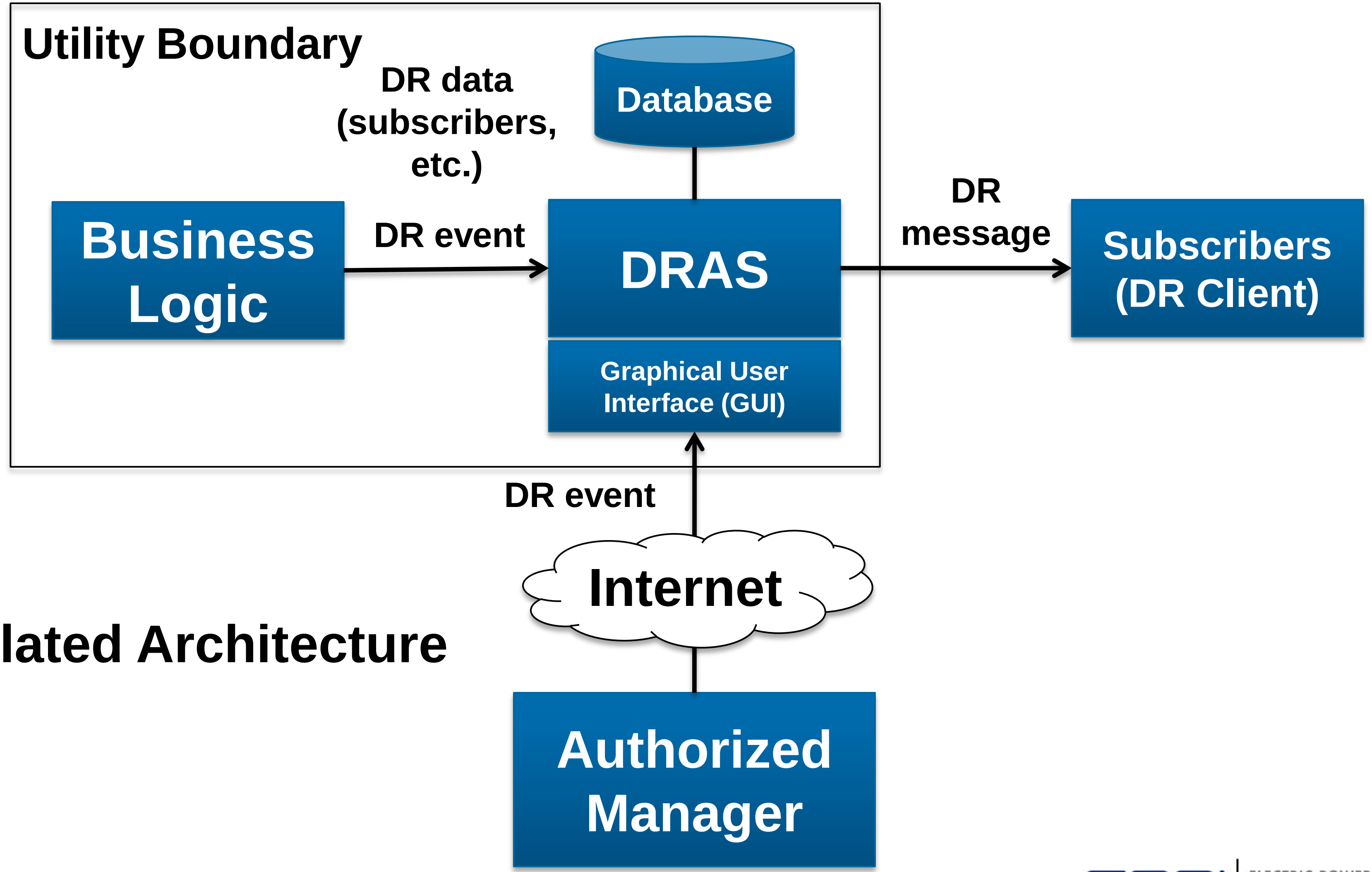
A threat agent unintentionally or maliciously modifies the DRAS configuration to send (or not send) DR messages at incorrect times and to incorrect devices. This could deliver a wrong, but seemingly legitimate set of messages to the customer system.

Assumptions

- DRAS issues a DR message when receiving DR event information in the following ways:
  (1) Business Logic feeds DR event to DRAS automatically based on its analysis;
  (2) Authorized manager manually generates and feeds DR event to DRAS through management GUI.

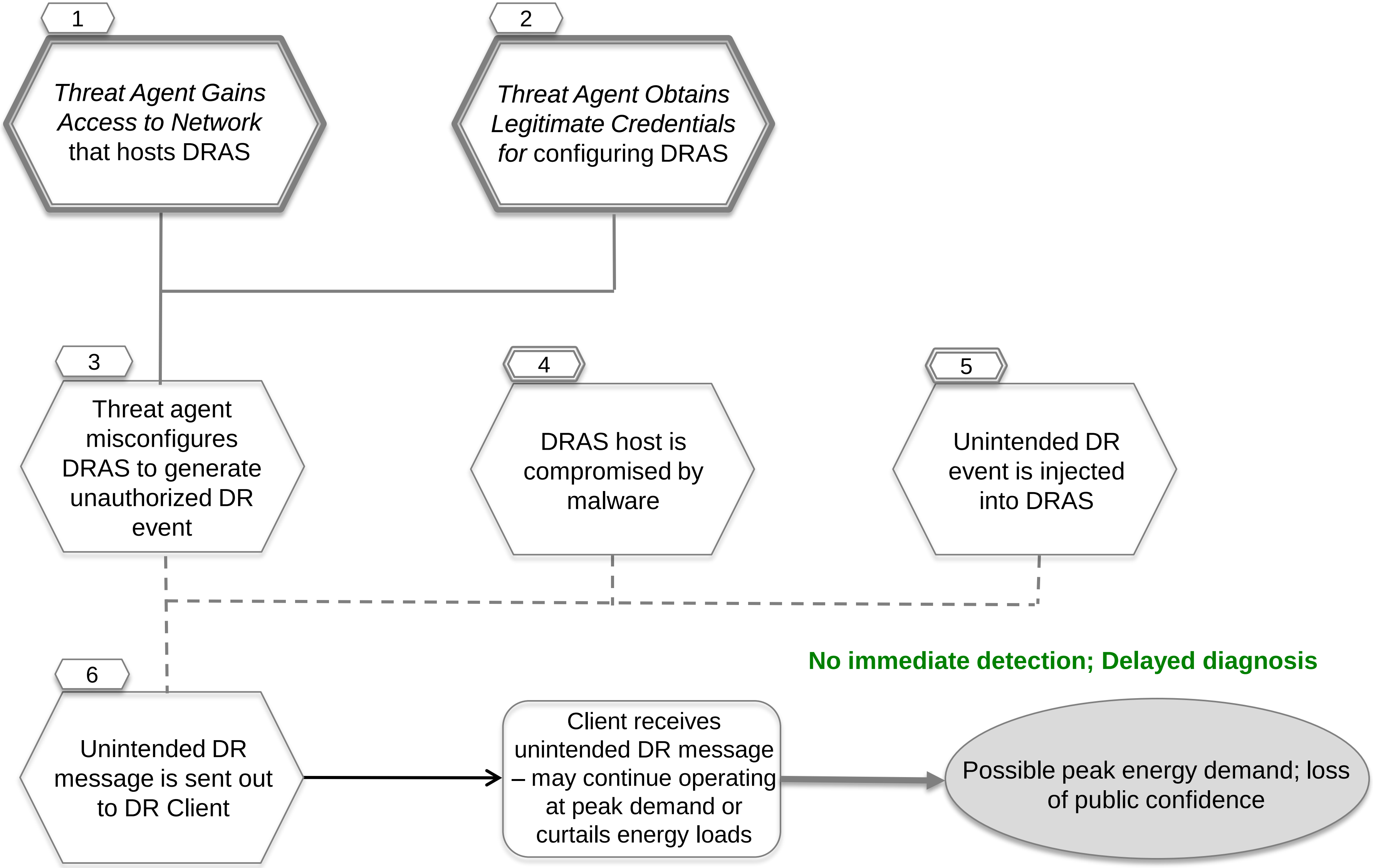
DR.4 Improper DRAS Configuration Causes Inappropriate DR Messages

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership



Related Architecture

DR.4 Improper DRAS Configuration Causes Inappropriate DR Messages (1/4)



1

Threat Agent Gains Access to Network that hosts DRAS

2

Threat Agent Obtains Legitimate Credentials for configuring DRAS

3

Threat agent misconfigures DRAS to generate unauthorized DR event

4

DRAS host is compromised by malware

5

Unintended DR event is injected into DRAS

No immediate detection; Delayed diagnosis

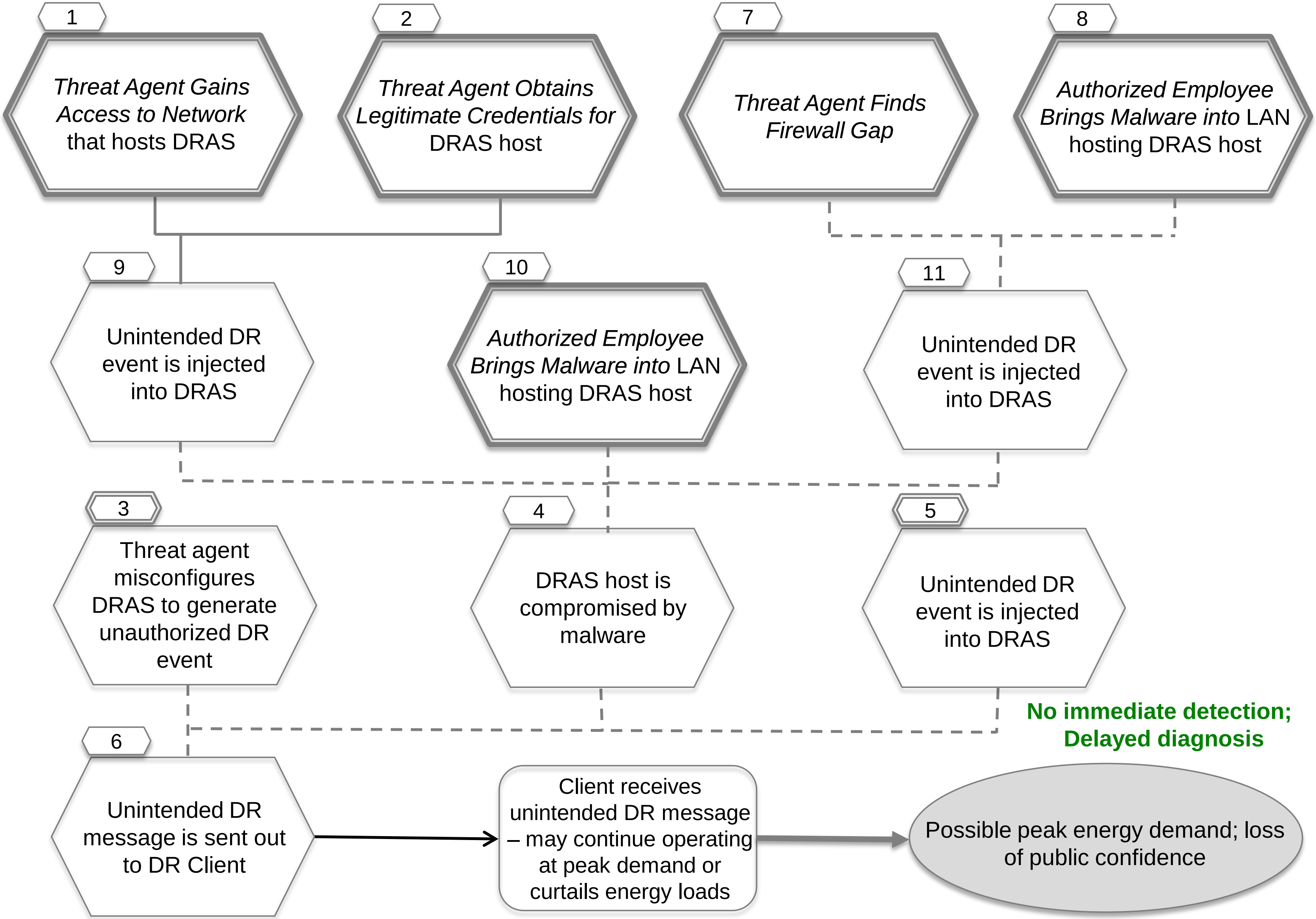
6

Unintended DR message is sent out to DR Client

Client receives unintended DR message – may continue operating at peak demand or curtails energy loads

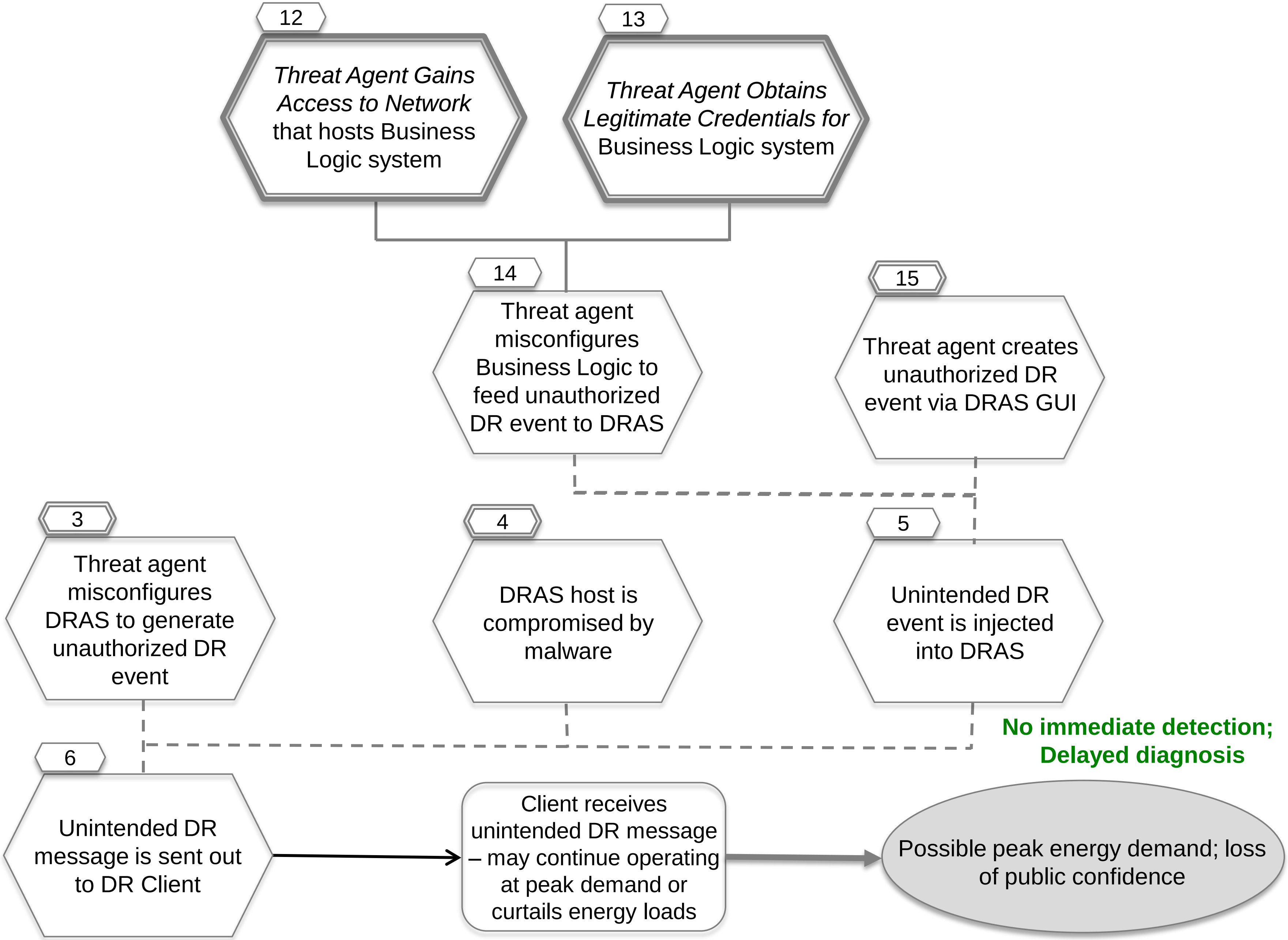
Possible peak energy demand; loss of public confidence

DR.4 Improper DRAS Configuration Causes Inappropriate DR Messages (2/4)


1
Threat Agent Gains Access to Network that hosts DRAS
2
Threat Agent Obtains Legitimate Credentials for DRAS host
7
Threat Agent Finds Firewall Gap
8
Authorized Employee Brings Malware into LAN hosting DRAS host
9
Unintended DR event is injected into DRAS
10
Authorized Employee Brings Malware into LAN hosting DRAS host
11
Unintended DR event is injected into DRAS
3
Threat agent misconfigures DRAS to generate unauthorized DR event
4
DRAS host is compromised by malware
5
Unintended DR event is injected into DRAS
6
Unintended DR message is sent out to DR Client
Client receives unintended DR message – may continue operating at peak demand or curtails energy loads
Possible peak energy demand; loss of public confidence

No immediate detection; Delayed diagnosis

DR.4 Improper DRAS Configuration Causes Inappropriate DR Messages (3/4)



12 *Threat Agent Gains Access to Network* that hosts Business Logic system

13 *Threat Agent Obtains Legitimate Credentials for* Business Logic system

14 Threat agent misconfigures Business Logic to feed unauthorized DR event to DRAS

15 Threat agent creates unauthorized DR event via DRAS GUI

3 Threat agent misconfigures DRAS to generate unauthorized DR event

4 DRAS host is compromised by malware

5 Unintended DR event is injected into DRAS

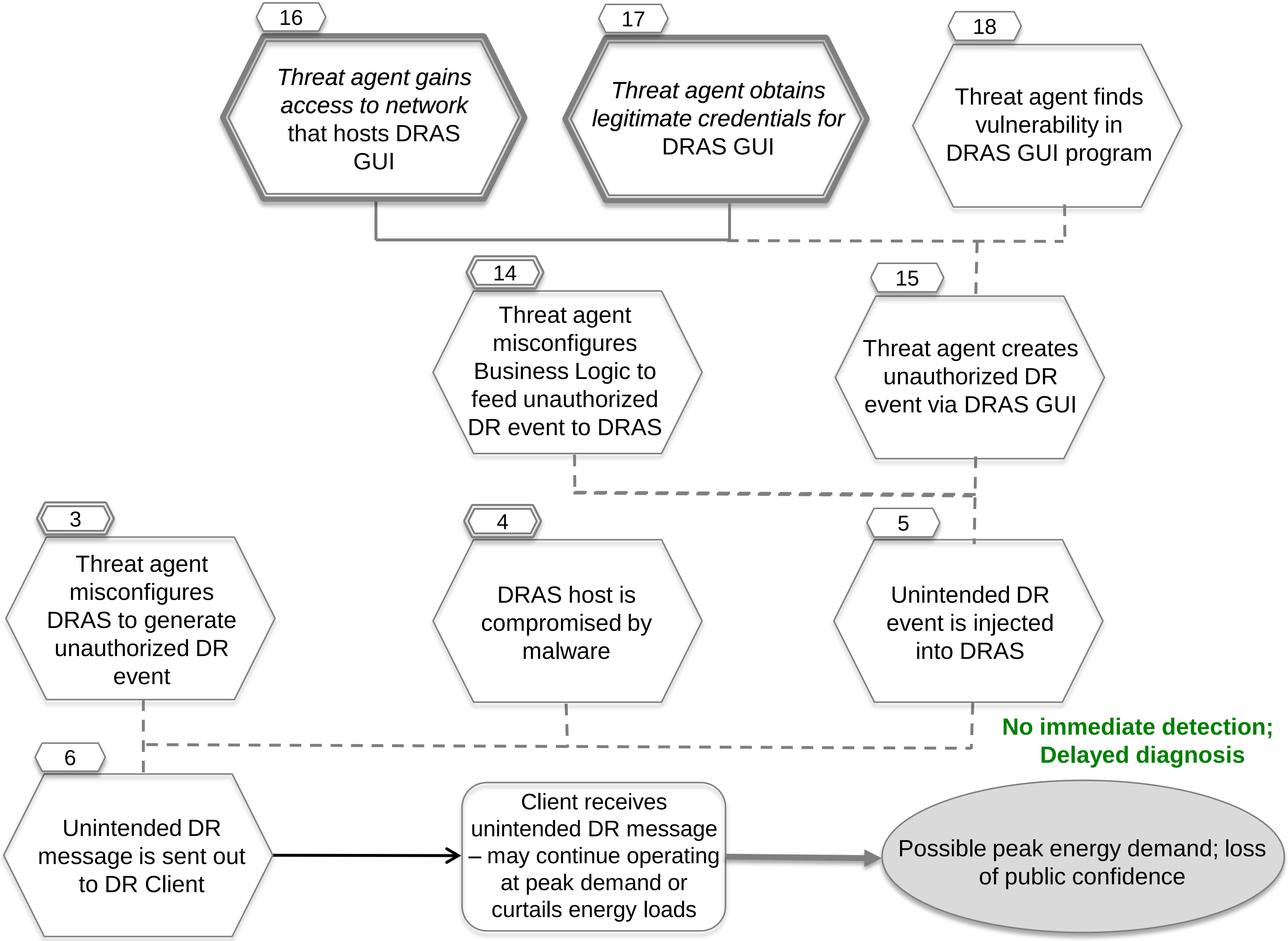
6 Unintended DR message is sent out to DR Client

Client receives unintended DR message – may continue operating at peak demand or curtails energy loads

Possible peak energy demand; loss of public confidence

No immediate detection; Delayed diagnosis

DR.4 Improper DRAS Configuration Causes Inappropriate DR Messages (4/4)



16

Threat agent gains access to network that hosts DRAS GUI

17

Threat agent obtains legitimate credentials for DRAS GUI

18

Threat agent finds vulnerability in DRAS GUI program

14

Threat agent misconfigures Business Logic to feed unauthorized DR event to DRAS

15

Threat agent creates unauthorized DR event via DRAS GUI

3

Threat agent misconfigures DRAS to generate unauthorized DR event

4

DRAS host is compromised by malware

5

Unintended DR event is injected into DRAS

No immediate detection; Delayed diagnosis

6

Unintended DR message is sent out to DR Client

Client receives unintended DR message – may continue operating at peak demand or curtails energy loads

Possible peak energy demand; loss of public confidence

DR.4 Improper DRAS Configuration Causes Inappropriate DR Messages

Potential Mitigations

1 - See common sub tree *Threat Agent Gains Access to Network <specific network>*

2 - See common sub tree *Threat Agent Obtains Legitimate Credentials for <system or function>*

3 - *Generate alerts* on changes to configurations on DRAS; *Detect unauthorized configuration changes*; *Create audit log* of DR messages generated; *Require second-level authentication* to change configuration

5, 6 - *Validate inputs*, specifically the reasonableness of DR event

7 - See common sub tree *Threat Agent Finds Firewall Gap*

8 - See common sub tree *Authorized Employee Brings Malware into <system or network>*

9, 11 - *Require application whitelisting*

11 - *Conduct penetration testing*; *Perform security testing*; *Maintain patches* in DRAS host; *Maintain anti-virus*

DR.4 Improper DRAS Configuration Causes Inappropriate DR Messages

Potential Mitigations (2)

13 - See common sub tree *Threat Agent Obtains Legitimate Credentials for <system or function>*

14 - *Use RBAC* to limit generation of DR event; *Generate alerts* on changes to configurations on Business Logic; *Detect unauthorized configuration changes*; *Create audit log* of DR events generated

15 - *Create audit log* of DR events generated; *Generate alarm* on unexpected DR event generation

18 - *Maintain patches* in DRAS GUI host; *Maintain anti-virus*; *Detect unauthorized connections* to DRAS GUI; *Restrict Internet access* to DRAS GUI

DGM.11 Threat Agent Triggers Blackout via Remote Access

Description

A threat agent gains access to selected elements of the utility DMS system - which includes all distribution automation systems and equipment in control rooms, substations, and on pole tops - via remote connections. After gaining the required access, the threat agent manufactures an artificial cascade through sequential tripping of select critical feeders and components, causing automated tripping of generation sources due to power and voltage fluctuations.

Assumptions

- Remote connections for vendor access are tightly controlled and physically disconnected when not in use, but inadvertent connections sometimes occur
- DMS/SCADA network segregated from corporate, public networks, no air gap
- Data logging is performed on DMS system, recording logins, breaker trips, capacitor bank switching, configuration changes, etc.

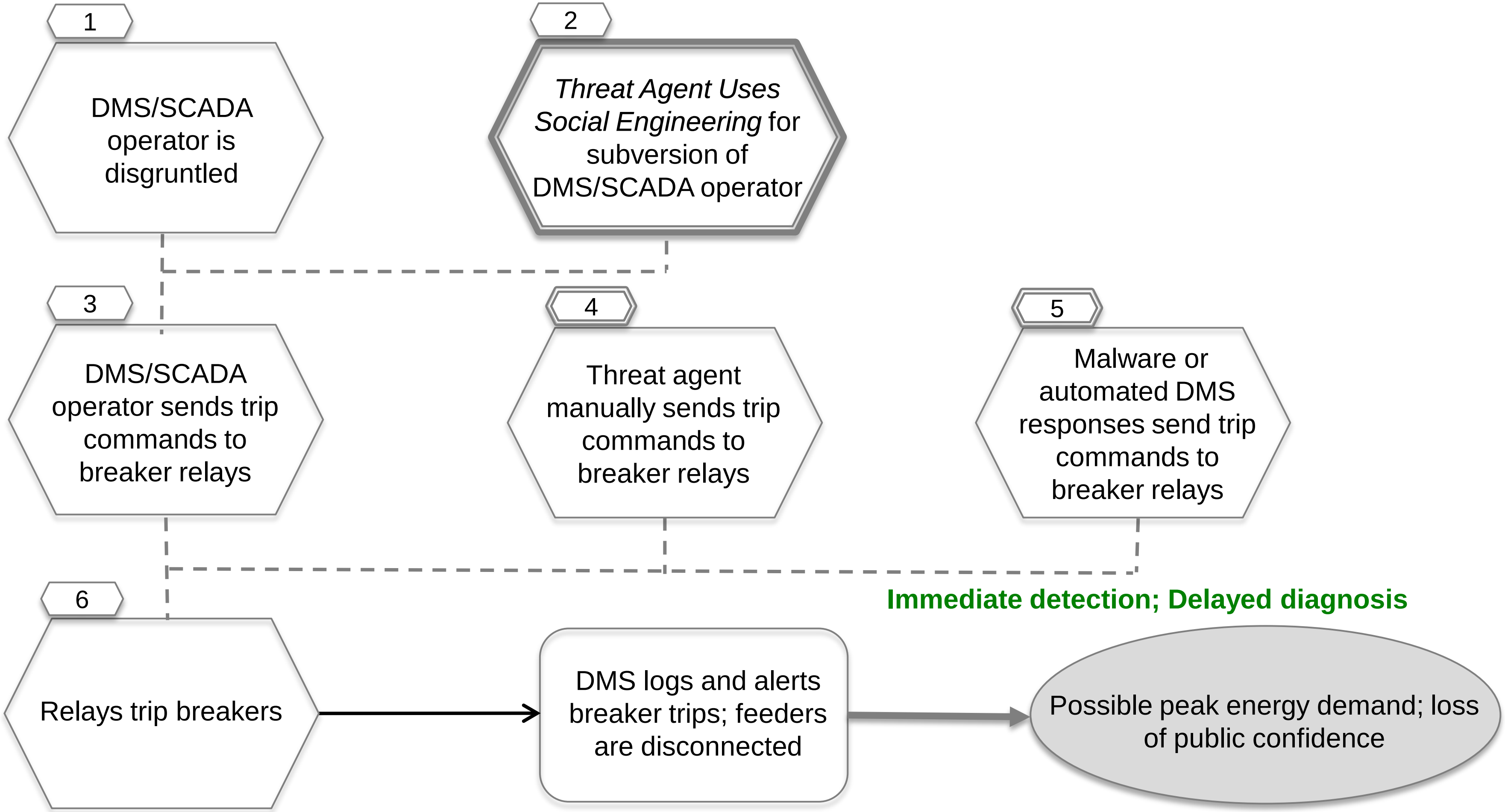
DGM.11 Threat Agent Triggers Blackout via Remote Access

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

Assumptions (2)

- Some DMS communications are run over leased fiber lines where some communication’s equipment is shared with other entities
- Intrusion detection systems are not present on DMS network
- Electrical infrastructure information resides on corporate networks as well as the control network
- Distribution communications do not employ encryption and defense in depth
- Moderate complexity password authentication, no two-factor authentication
- DMS/SCADA system is monitored 24/7 by dedicated control personnel
- Some utility linemen and communication personnel carry laptops that permit connections to DMS/SCADA field equipment, communication devices, and the DMS system over the control system network
- Control system network is flat
- Distribution system is largely radial with tie lines at the end of some laterals

DGM.11 Threat Agent Triggers Blackout via Remote Access to Distribution System (1/4)



1

DMS/SCADA operator is disgruntled

2

Threat Agent Uses Social Engineering for subversion of DMS/SCADA operator

3

DMS/SCADA operator sends trip commands to breaker relays

4

Threat agent manually sends trip commands to breaker relays

5

Malware or automated DMS responses send trip commands to breaker relays

Immediate detection; Delayed diagnosis

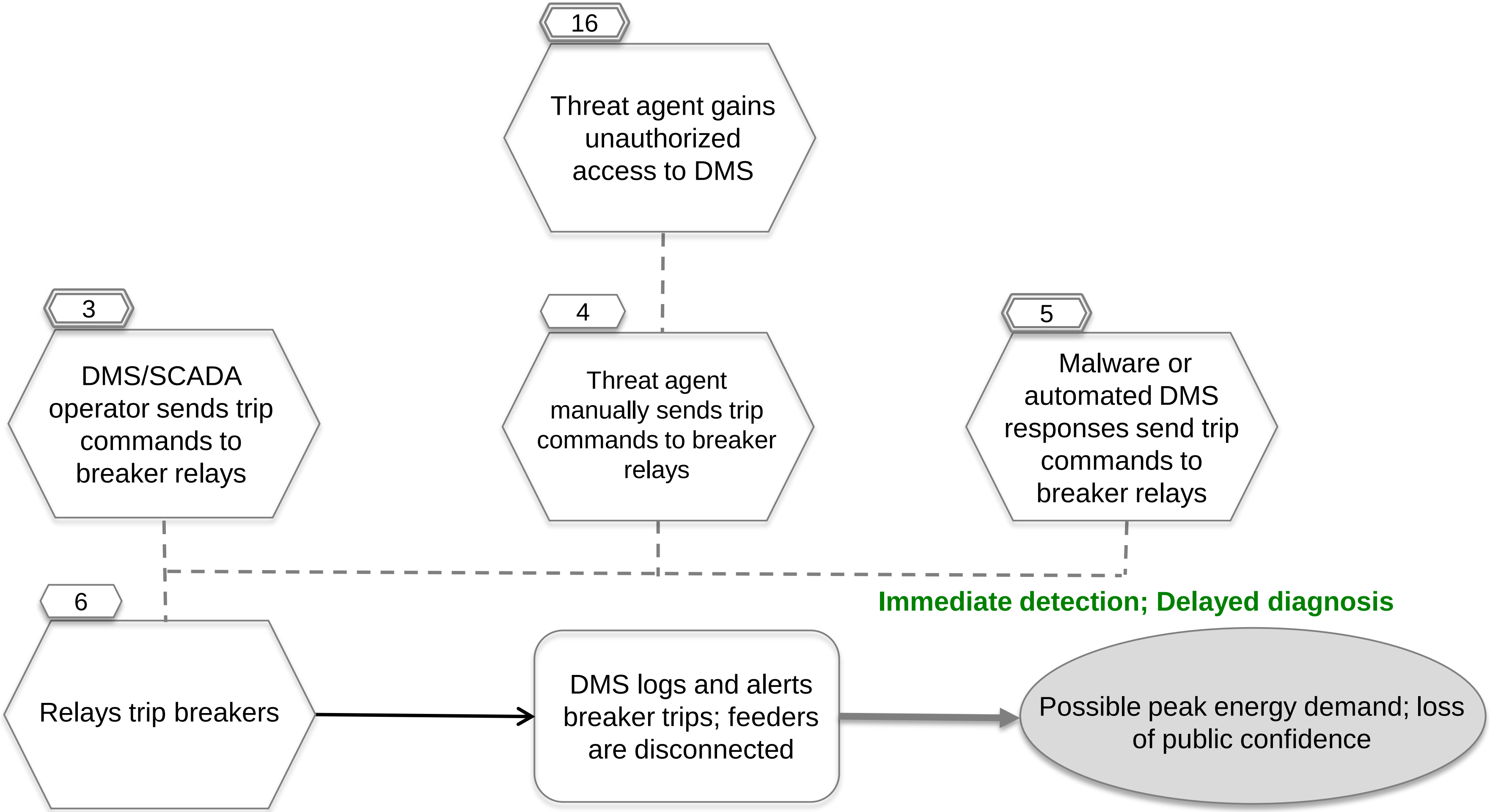
6

Relays trip breakers

DMS logs and alerts breaker trips; feeders are disconnected

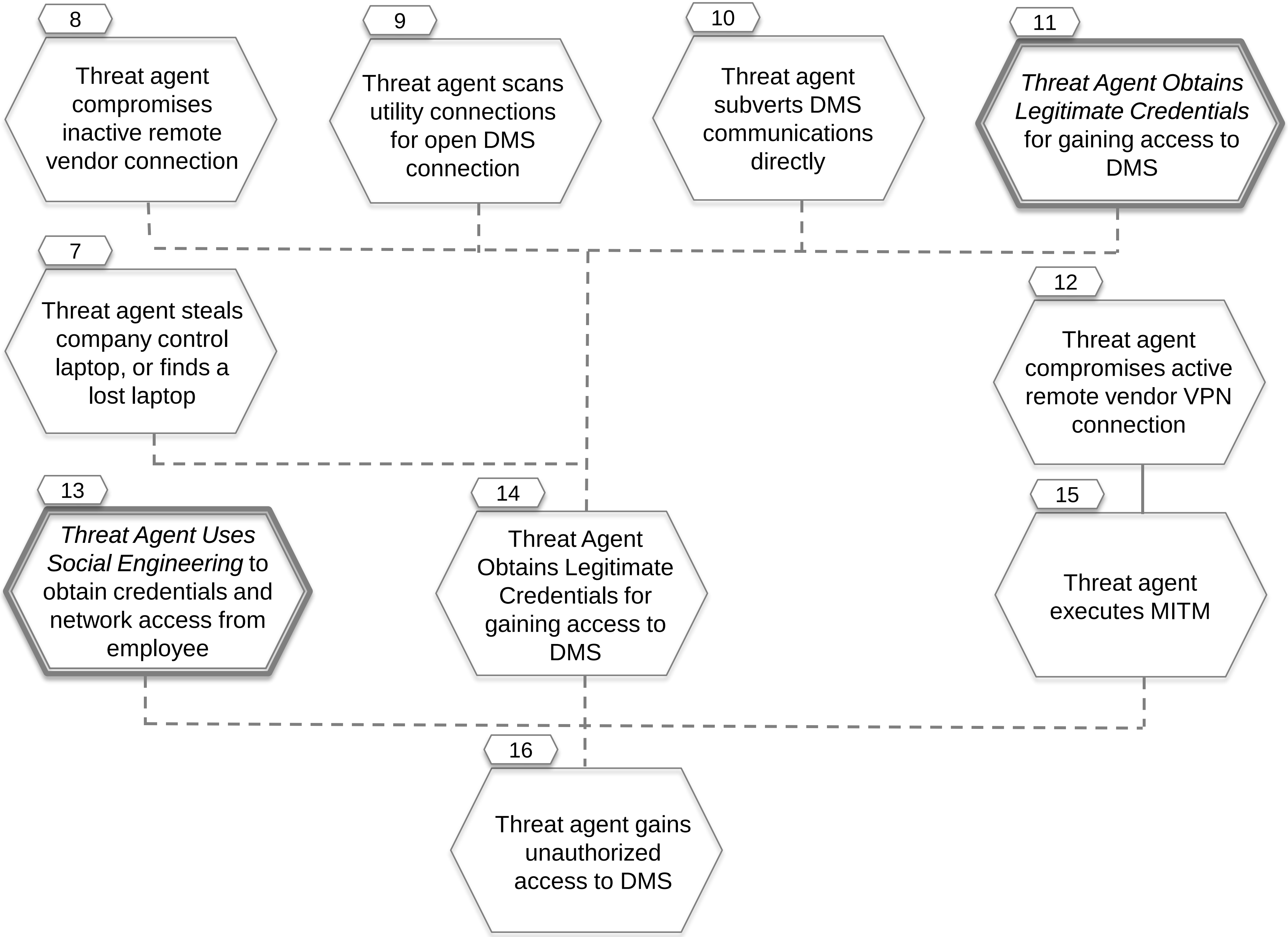
Possible peak energy demand; loss of public confidence

DGM.11 Threat Agent Triggers Blackout via Remote Access to Distribution System (2/4)



16
Threat agent gains unauthorized access to DMS
3
DMS/SCADA operator sends trip commands to breaker relays
4
Threat agent manually sends trip commands to breaker relays
5
Malware or automated DMS responses send trip commands to breaker relays
6
Relays trip breakers
Immediate detection; Delayed diagnosis
DMS logs and alerts breaker trips; feeders are disconnected
Possible peak energy demand; loss of public confidence

DGM.11 Threat Agent Triggers Blackout via Remote Access to Distribution System (3/4)



8 Threat agent compromises inactive remote vendor connection

9 Threat agent scans utility connections for open DMS connection

10 Threat agent subverts DMS communications directly

11 *Threat Agent Obtains Legitimate Credentials* for gaining access to DMS

7 Threat agent steals company control laptop, or finds a lost laptop

12 Threat agent compromises active remote vendor VPN connection

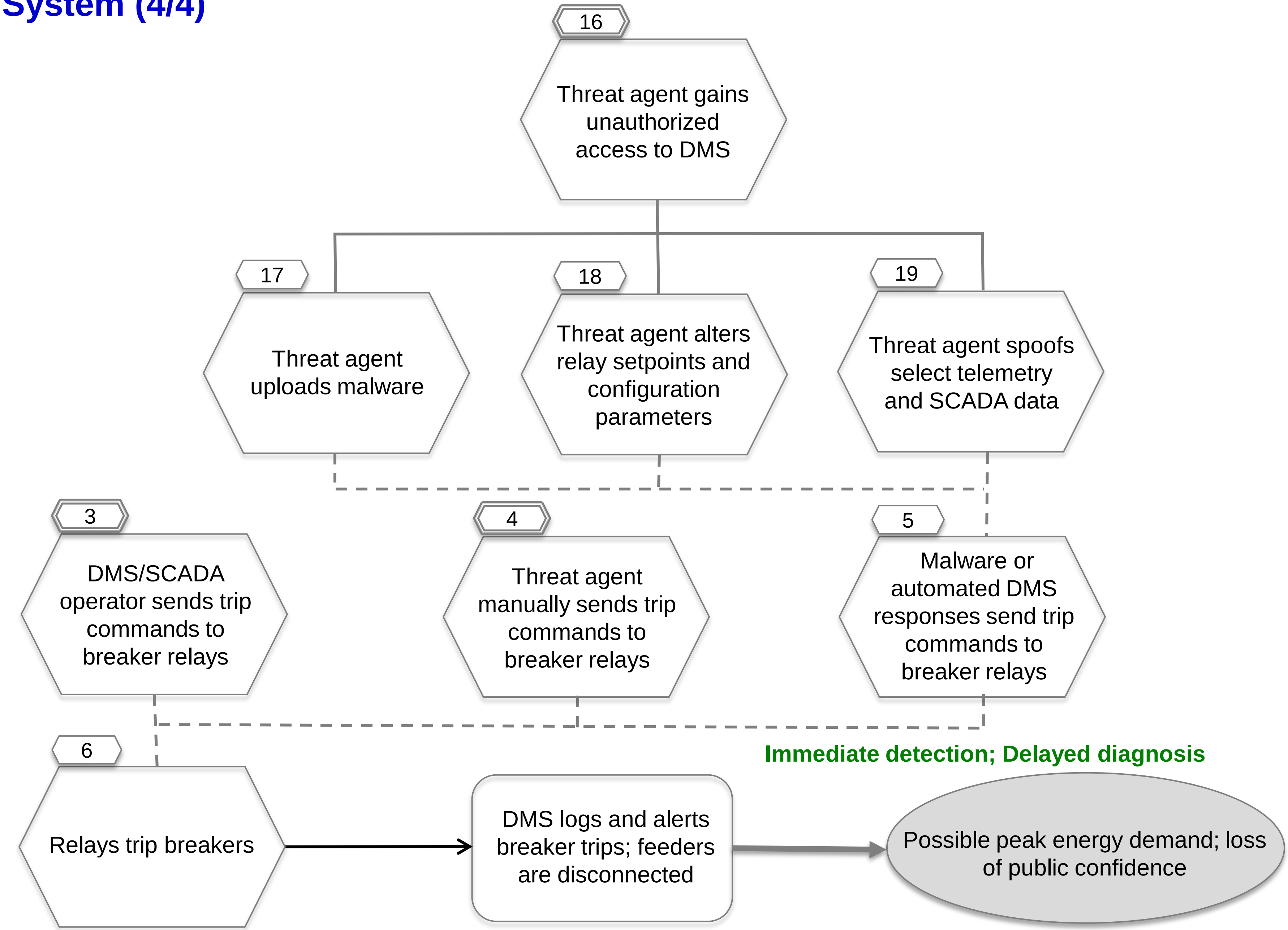
13 *Threat Agent Uses Social Engineering* to obtain credentials and network access from employee

14 Threat Agent Obtains Legitimate Credentials for gaining access to DMS

15 Threat agent executes MITM

16 Threat agent gains unauthorized access to DMS

DGM.11 Threat Agent Triggers Blackout via Remote Access to Distribution System (4/4)


16
Threat agent gains unauthorized access to DMS
17
Threat agent uploads malware
18
Threat agent alters relay setpoints and configuration parameters
19
Threat agent spoofs select telemetry and SCADA data
3
DMS/SCADA operator sends trip commands to breaker relays
4
Threat agent manually sends trip commands to breaker relays
5
Malware or automated DMS responses send trip commands to breaker relays
6
Relays trip breakers
DMS logs and alerts breaker trips; feeders are disconnected
Immediate detection; Delayed diagnosis
Possible peak energy demand; loss of public confidence

DGM.11 Threat Agent Triggers Blackout via Remote Access

Potential Mitigations

1 - *Verify personnel* by performing thorough background checks

2 - See common sub tree *Threat Agent Uses Social Engineering*

7 - Training on security for portable devices

7, 10 - *Restrict physical access* to DMS equipment

8 - *Restrict remote access* of vendor connections

8, 10, 11, 14 - *Encrypt* all DMS/SCADA communications

9, 10 - *Minimize functions* on control system equipment by disabling all unused ports

11 - See common sub tree *Threat Agent Obtains Legitimate Credentials*

14 - *Require strong passwords* or *two-factor authentication*

16 - *Require intrusion detection* on DMS networks/hosts

16 - *Restrict remote access* (vendors) by installing patches and updates via physical media mailed by vendor instead of allowing remote vendor access

DGM.11 Threat Agent Triggers Blackout via Remote Access

Potential Mitigations (2)

16, 19 - *Encrypt* and authenticate all DMS/SCADA communications

17 - *Check integrity* of firmware, applications, patches, and updates

18 - *Authenticate users* of relays using strong passwords that are different for each relay

19 - *Restrict physical access* to telemetry and communication equipment

Common Sub Trees

- Threat Agent Gains Capability to Reconfigure <firewall>
- Threat Agent Blocks Wireless Communication Channel Connecting <x and y>
- Authorized Employee Brings Malware into <system or network>
- Threat Agent Obtains Legitimate Credentials for <system or function>
- Threat Agent Uses Social Engineering to <desired outcome>
- Threat Agent Finds Firewall Gap <specific firewall>
- Threat Agent Steals <file>
- Threat Agent Gains Access to <network>

Common Tree: Threat Agent Gains Capability to Reconfigure <firewall>

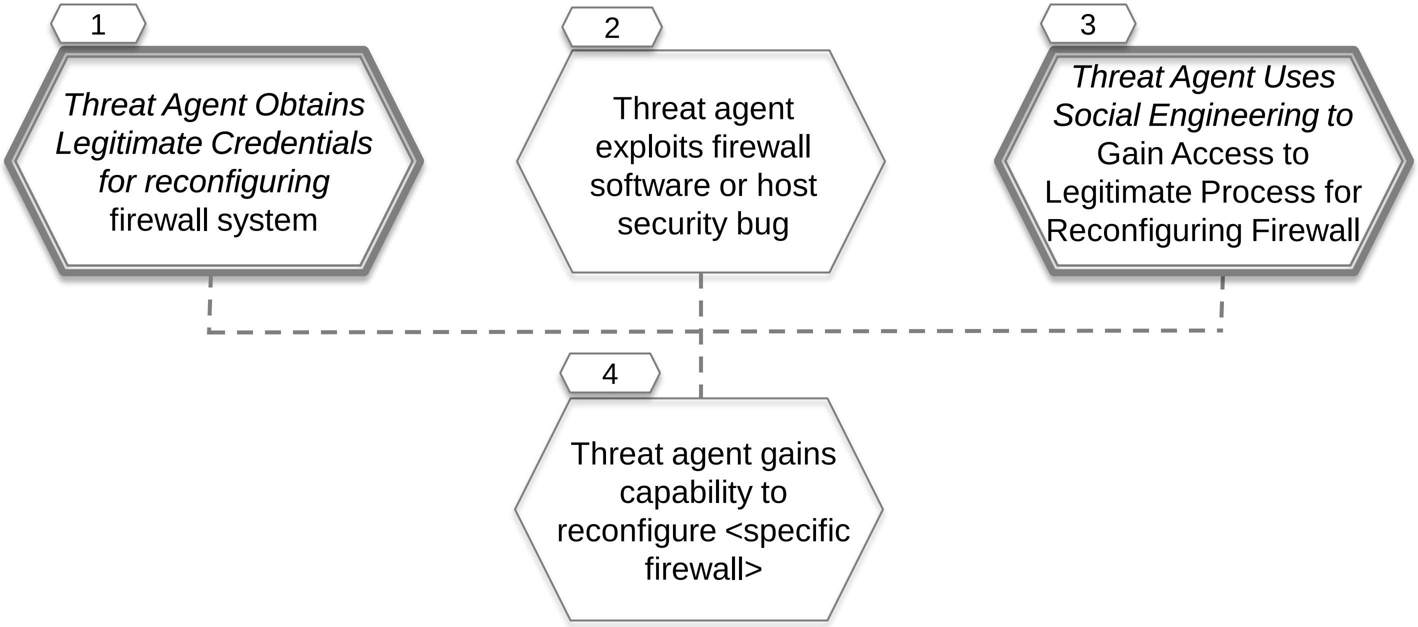
Description

A threat agent gains the capability to change firewall rules on a specific firewall to permit types of traffic to flow through the firewall that will enable future attacks.

Assumptions

- Threat agent has access to a network to which the firewall has an interface.

Common Tree: Threat Agent Gains Capability to Reconfigure <firewall>



1

Threat Agent Obtains Legitimate Credentials for reconfiguring firewall system

2

Threat agent exploits firewall software or host security bug

3

Threat Agent Uses Social Engineering to Gain Access to Legitimate Process for Reconfiguring Firewall

4

Threat agent gains capability to reconfigure <specific firewall>

Common Tree: Threat Agent Gains Capability to Reconfigure <firewall>

Potential Mitigations

1 - See common sub tree *Threat Agent Obtains Legitimate Credentials* for <system or function>

2 - *Conduct penetration testing* to uncover firewall vulnerabilities

2 - *Implement configuration management* in a strict manner for the firewall system

2 - *Maintain patches* on firewall system

2 - Detect unauthorized access through traffic monitoring, specifically to detect reconnaissance

2 - *Require intrusion detection and prevention*

2 - Create audit log of attempts to access firewall host

2 - *Require authentication* for system and database access for firewall

2 - *Restrict database access on firewall* to authorized applications and/or locally authenticated users

3 - See common sub tree *Threat Agent Uses Social Engineering* to <desired outcome>

Common Tree: Threat Agent Blocks Wireless Channel Connecting <x and y>

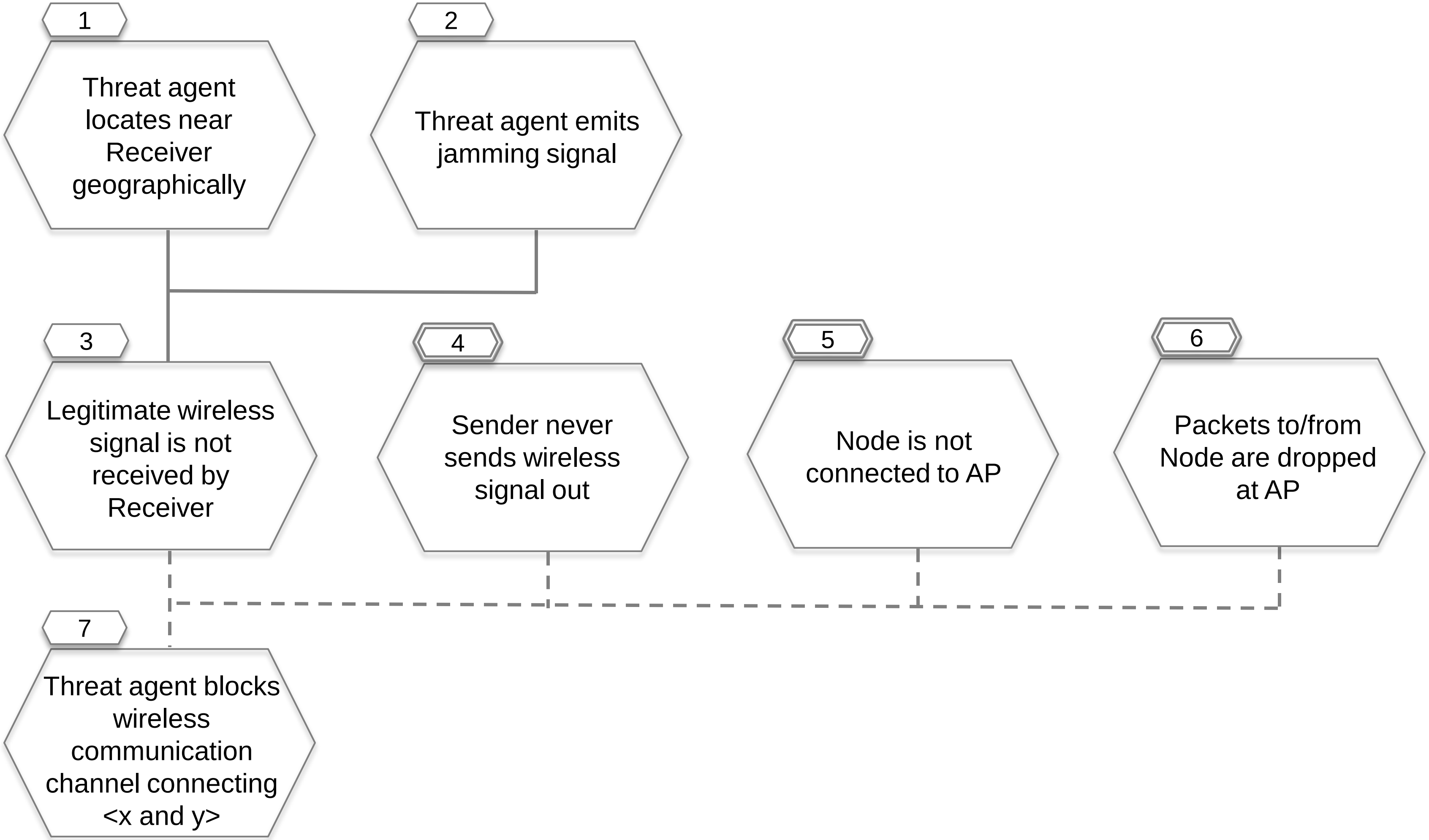
Description

The threat agent stops the flow of messages on a wireless communication channel connecting two entities, or slows it down to a point that it is essentially stopped.

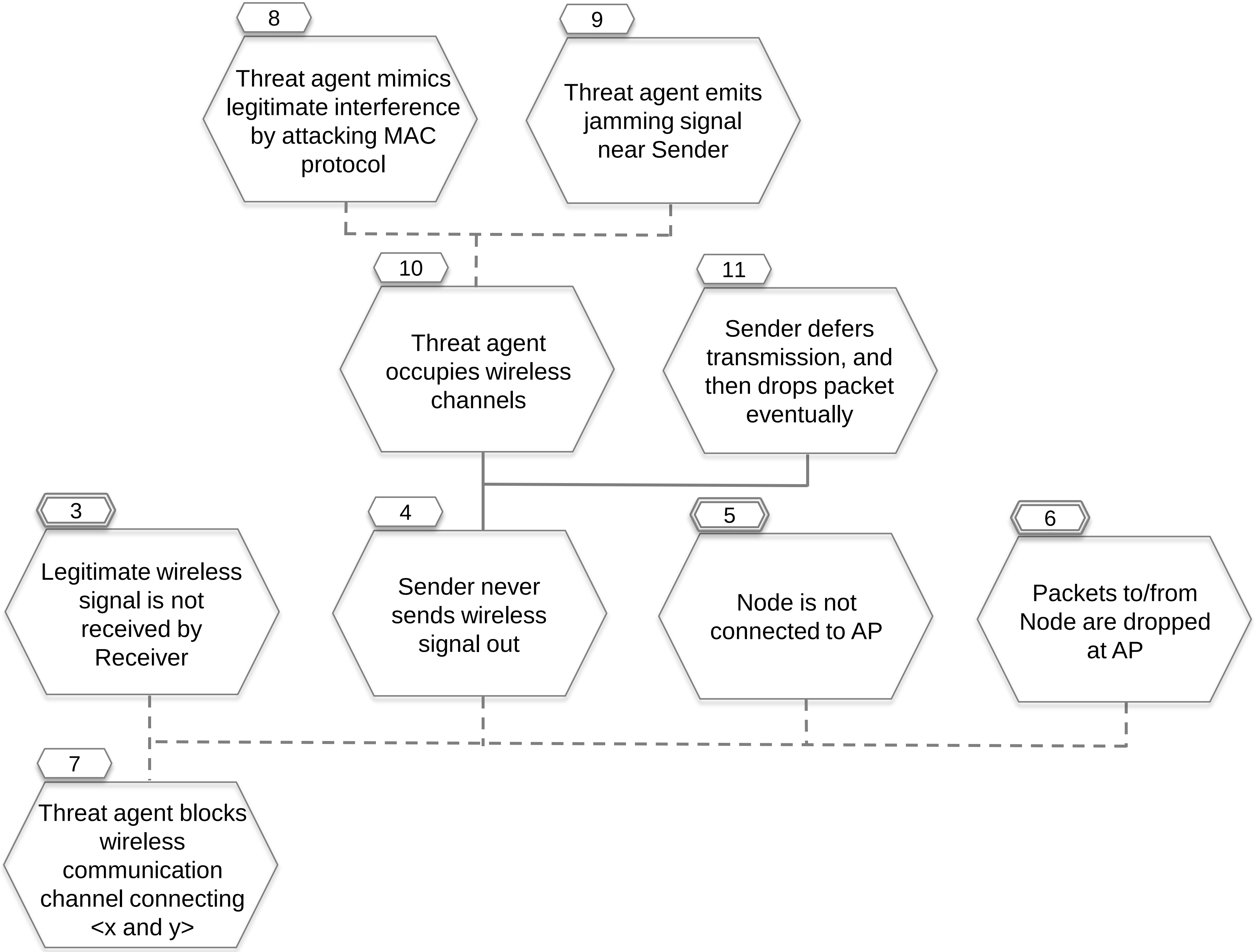
Assumptions

- The backbone network for this wireless channel is wired, e.g., the Internet. Thus, wireless communication connecting <x and y>, in fact, consists of two wireless channels in the access networks: node x - wireless Access Point (AP) and AP – node y. Assuming these two channels are functionally same, this common tree considers the wireless channel between AP and a node. The terms ‘sender’ and ‘receiver’ refer to the entity that sends and receives the wireless signal, respectively, which may be an AP or a node.

Common Tree: Threat Agent Blocks Wireless Communication Channel Connecting <x and y> (1/4)

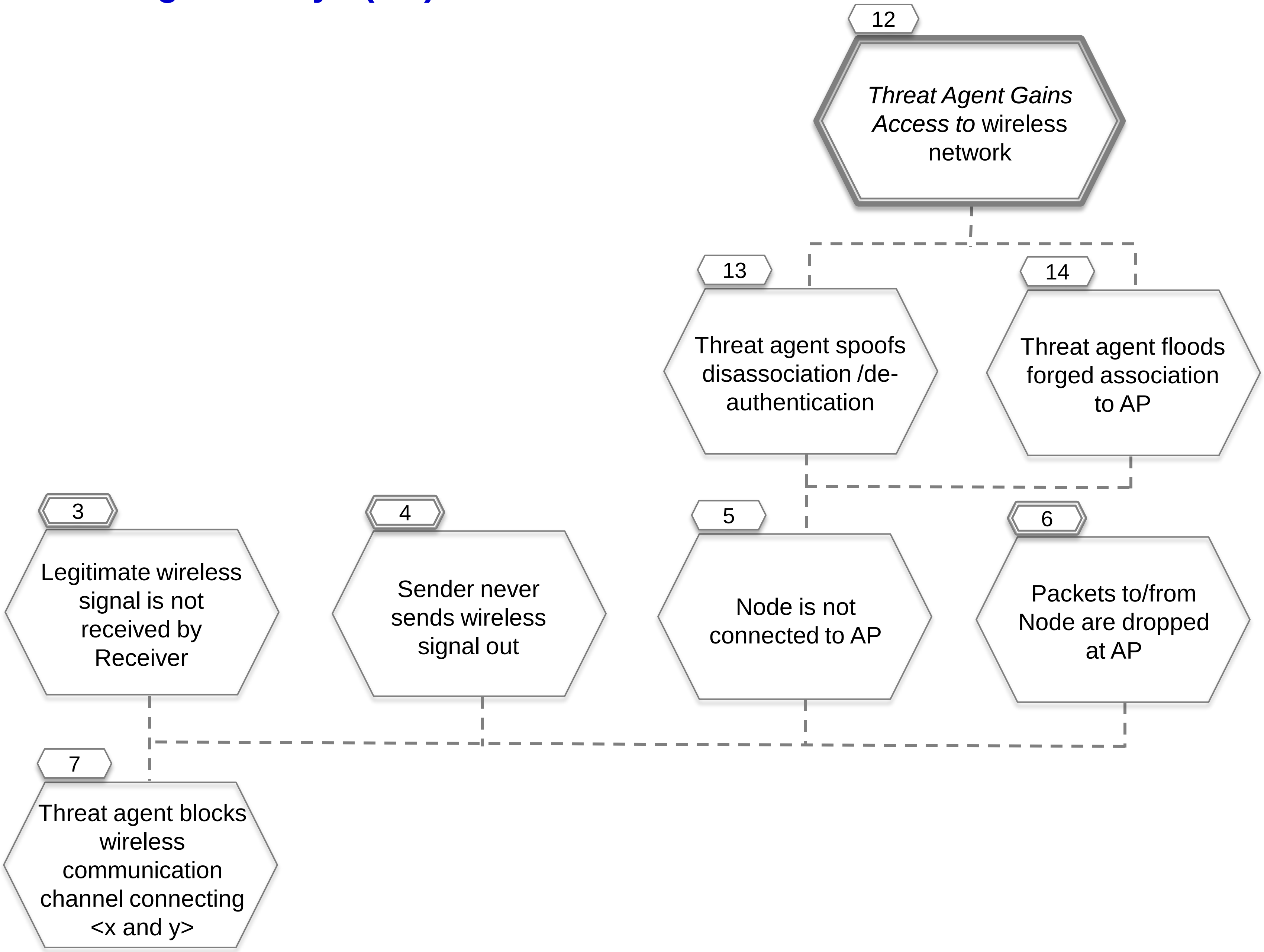

1
Threat agent locates near Receiver geographically
2
Threat agent emits jamming signal
3
Legitimate wireless signal is not received by Receiver
4
Sender never sends wireless signal out
5
Node is not connected to AP
6
Packets to/from Node are dropped at AP
7
Threat agent blocks wireless communication channel connecting <x and y>

Common Tree: Threat Agent Blocks Wireless Communication Channel Connecting <x and y> (2/4)

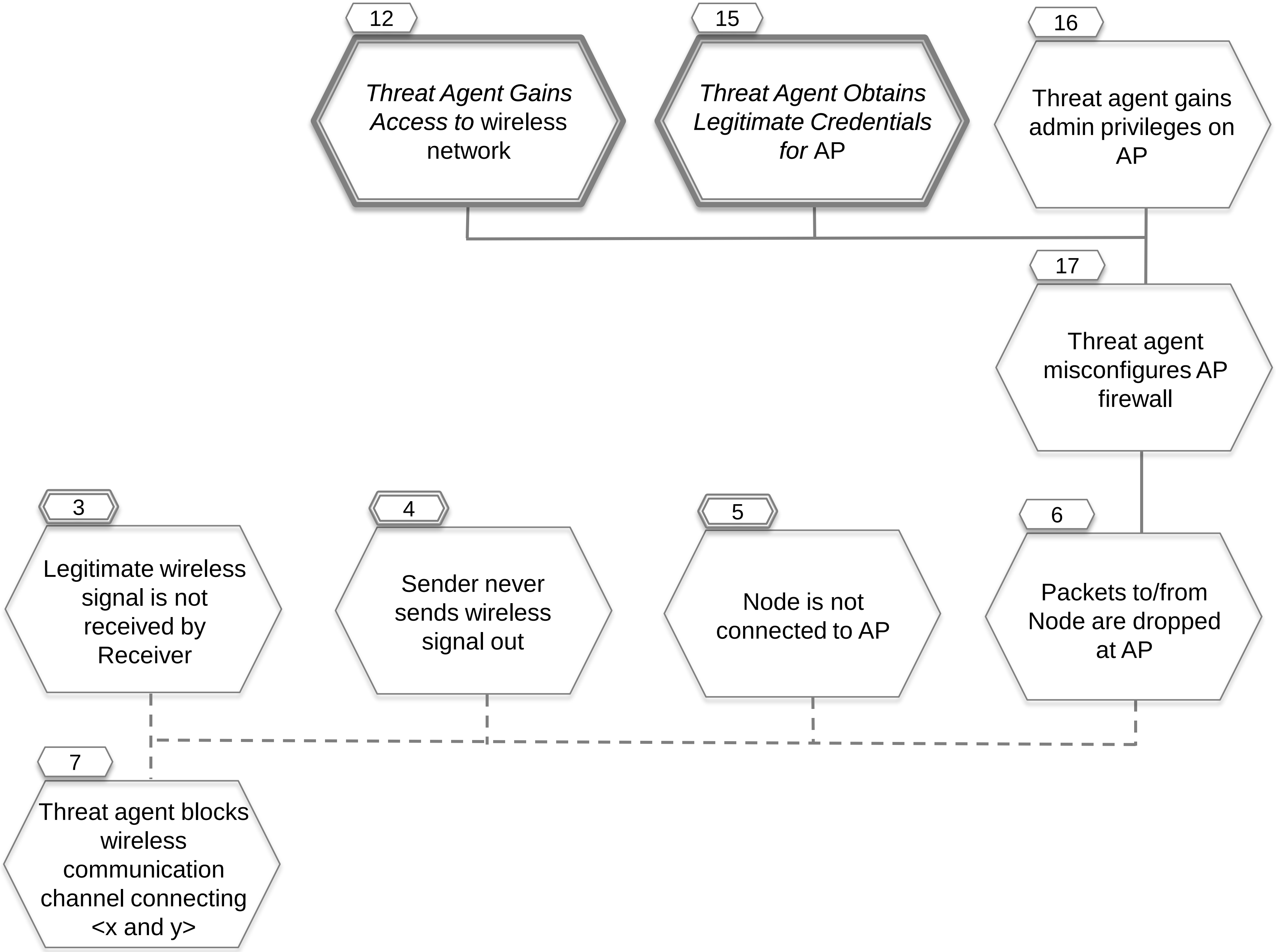


8
Threat agent mimics legitimate interference by attacking MAC protocol
9
Threat agent emits jamming signal near Sender
10
Threat agent occupies wireless channels
11
Sender defers transmission, and then drops packet eventually
3
Legitimate wireless signal is not received by Receiver
4
Sender never sends wireless signal out
5
Node is not connected to AP
6
Packets to/from Node are dropped at AP
7
Threat agent blocks wireless communication channel connecting <x and y>

Common Tree: Threat Agent Blocks Wireless Communication Channel Connecting <x and y> (3/4)


12
Threat Agent Gains Access to wireless network
13
Threat agent spoofs disassociation /de-authentication
14
Threat agent floods forged association to AP
3
Legitimate wireless signal is not received by Receiver
4
Sender never sends wireless signal out
5
Node is not connected to AP
6
Packets to/from Node are dropped at AP
7
Threat agent blocks wireless communication channel connecting <x and y>

Common Tree: Threat Agent Blocks Wireless Communication Channel Connecting <x and y> (4/4)


12
Threat Agent Gains Access to wireless network
15
Threat Agent Obtains Legitimate Credentials for AP
16
Threat agent gains admin privileges on AP
17
Threat agent misconfigures AP firewall
3
Legitimate wireless signal is not received by Receiver
4
Sender never sends wireless signal out
5
Node is not connected to AP
6
Packets to/from Node are dropped at AP
7
Threat agent blocks wireless communication channel connecting <x and y>

Common Tree: Threat Agent Blocks Wireless Channel Connecting <x and y>

Potential Mitigations

1 - *Restrict physical access* to AP and nodes

2 - *Detect unusual patterns* on wireless channel; *Generate alarm* on detection

3 - *Isolate network* for specific service; *Require spread-spectrum radio*; *Create audit logs* for network connectivity

4 - *Create audit logs* for network connectivity; *Generate alarm* on network disconnectivity

5 - *Generate alarm* on network disconnectivity

6 – *Require acknowledgment* for message transmission; *Require redundancy* of communication channel to ensure message delivery

9 - *Restrict physical access* to Sender; *Detect unusual patterns* on wireless channel; *Generate alarm* on detection

11 - *Create audit logs* for transmission failure rate

12 - See common sub tree *Threat Agent Gains Access to <network>*

Common Tree: Threat Agent Blocks Wireless Channel Connecting <x and y>

Potential Mitigations (2)

13 - *Detect unusual patterns* on association and authentication for wireless communication

14 - *Generate alarm* on detection of abnormal association delay

15 - See common sub tree *Threat Agent Obtains Legitimate Credentials for <system or function>*

16 - *Restrict remote access*; *Detect unauthorized access*; *Require multi-factor authentication*; *Enforce least privilege*

17 - *Generate alerts* on changes to configurations on AP; *Detect unauthorized configuration changes*; *Enforce restrictive firewall rules*

Common Tree: Authorized Employee Brings Malware into <system or network>

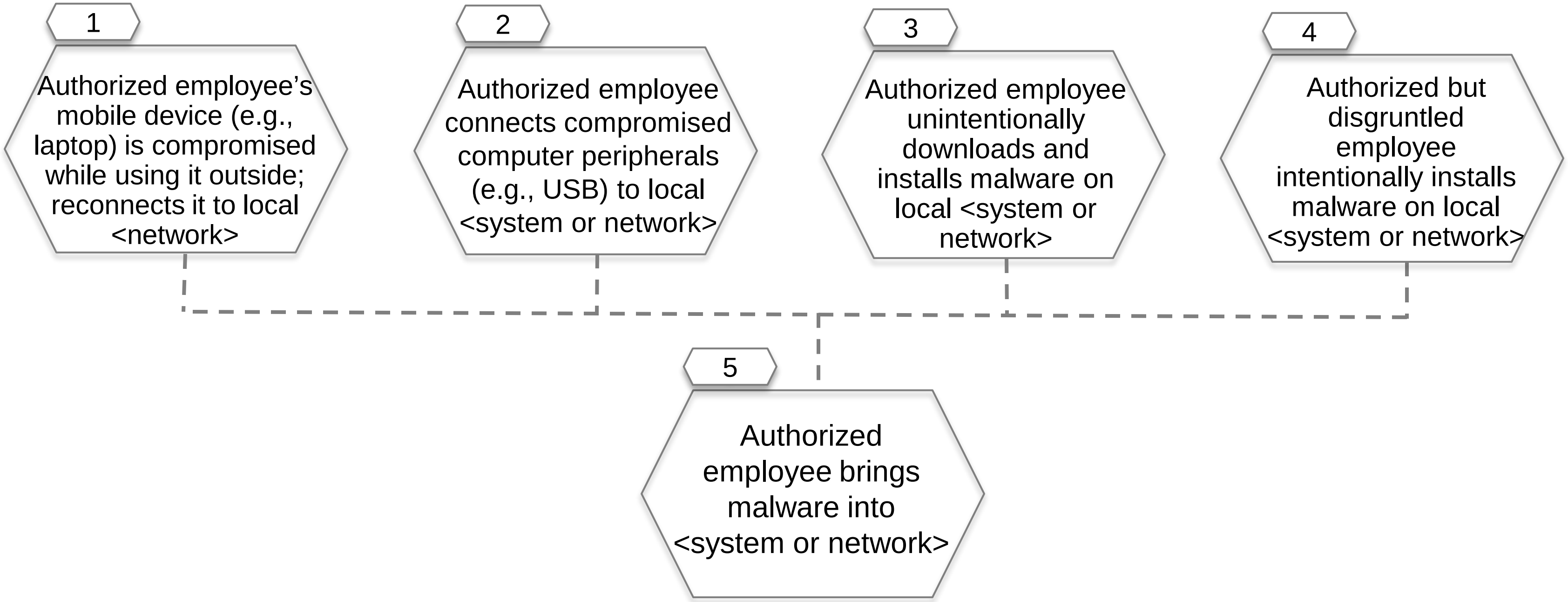
Description

An authorized employee uses the IT infrastructure to perform any action that results in the introduction of a particular piece of malware onto a specific network or a system.

Assumptions

- The network under discussion is protected by perimeter security tools (e.g., enterprise firewall), and communications within the local network is less restricted (e.g., no port number filtering and IP address filtering). Once a compromised device is connected to the local network, the malware may infect other systems in the network to compromise them. It is possible that a compromised device is under control a from threat agent remotely.

Common Tree: Authorized Employee Brings Malware into <system or network>


1
Authorized employee's mobile device (e.g., laptop) is compromised while using it outside; reconnects it to local <network>
2
Authorized employee connects compromised computer peripherals (e.g., USB) to local <system or network>
3
Authorized employee unintentionally downloads and installs malware on local <system or network>
4
Authorized but disgruntled employee intentionally installs malware on local <system or network>
5
Authorized employee brings malware into <system or network>

Common Tree: Authorized Employee Brings Malware into <system or network>

Potential Mitigations

1, 2 - *Create policy* regarding connection of mobile devices and peripherals to the network; *Test for malware* before connecting mobile device or peripheral to local network

1,2,3 - *Train personnel* regarding possible paths for infection to internal network

1,2,3,4 - *Maintain patches* on all systems; *Maintain anti-virus* on all systems

4 - *Verify personnel* to find any previous actions against employers

5 - *Require intrusion detection and prevention*

Common Tree: Threat Agent Obtains Legitimate Credentials <system or function>

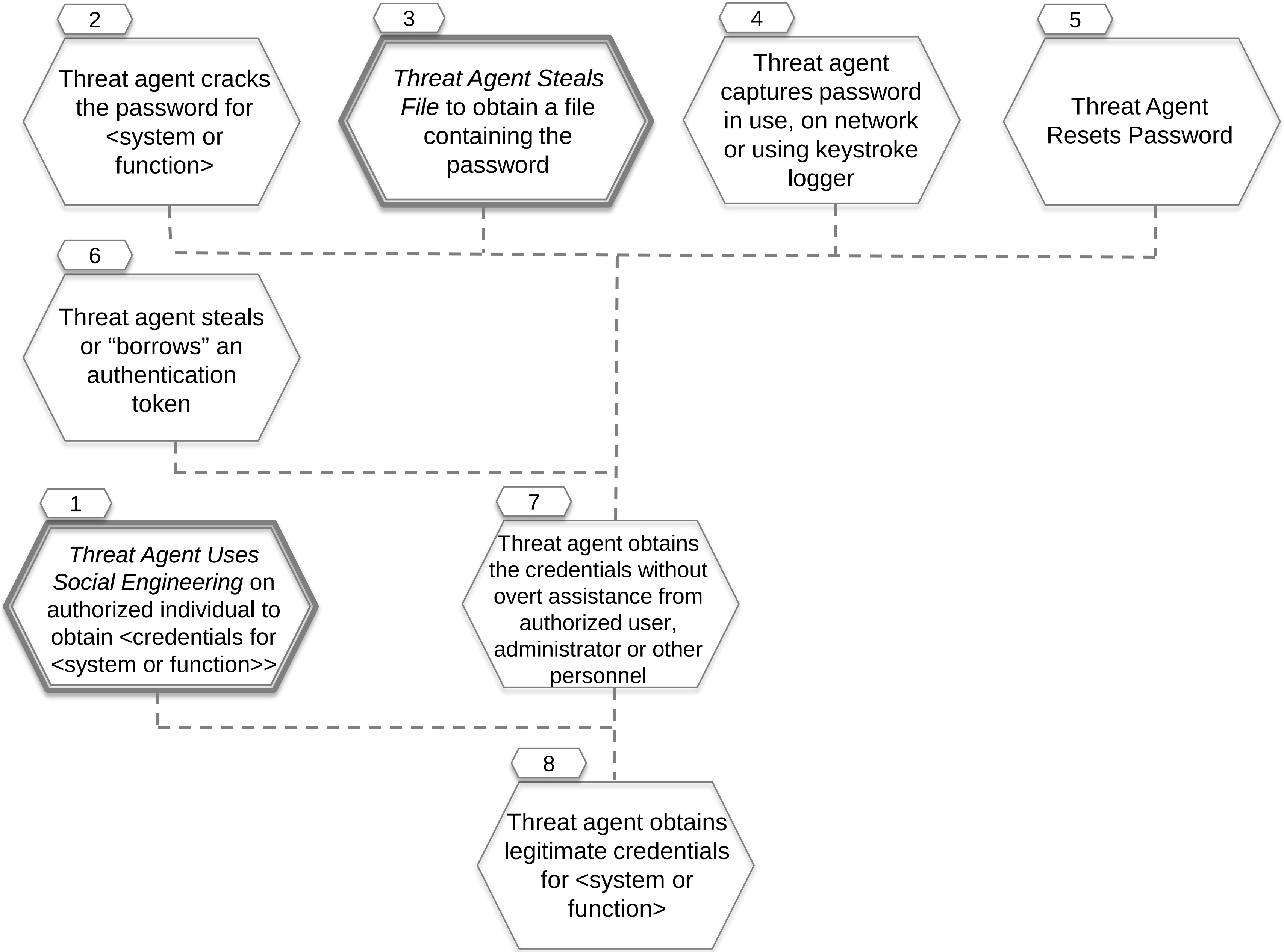
Description

A threat agent may gain legitimate credentials for a system, or credentials that provide privileges to perform specific functions, in a number of ways. This includes finding them, stealing them, guessing them, or changing them. The threat agent may use social engineering techniques to carry out these methods. Each technology and implementation used for credentials is resistant to some methods and susceptible to others.

Assumptions

- Credentials used are either any static piece of data (referred to as a password) OR a physical object (such as a key card, referred to as a token)
- These are common forms of one-factor authentication. If two-factor authentication is used, such as a token with a PIN, the adversary must take more, similar steps to obtain all “factors” of the credentials.
- Other types of authentication exist, but are not in scope for this tree. They could be similarly analyzed

Common Tree: Threat Agent Obtains Legitimate Credentials <system or function>


2
Threat agent cracks the password for <system or function>
3
Threat Agent Steals File to obtain a file containing the password
4
Threat agent captures password in use, on network or using keystroke logger
5
Threat Agent Resets Password
6
Threat agent steals or “borrows” an authentication token
1
Threat Agent Uses Social Engineering on authorized individual to obtain <credentials for <system or function>>
7
Threat agent obtains the credentials without overt assistance from authorized user, administrator or other personnel
8
Threat agent obtains legitimate credentials for <system or function>

Common Tree: Threat Agent Obtains Legitimate Credentials <system or function>

Potential Mitigations

1 - See common sub tree *Threat Agent Uses Social Engineering to obtain <desired information or capability>*

2 - *Design for security* by using strong passwords

3 - See common sub tree *Threat Agent Steals File*

3 - *Design for security* by not recording passwords in log files

4 - *Test for malware* on user workstations

4 - *Design for security* by not sending passwords in the clear over the network

4 - *Encrypt communication paths* on the network

4 - *Protect against replay* on the network

5 - *Design for security* by using strong security questions and protect answers

6 - *Require multi-factor authentication* such as using a token with a PIN

6 - *Define policy* regarding reporting and revocation of missing tokens

Common Tree: Threat Agent Uses Social Engineering <desired outcome>

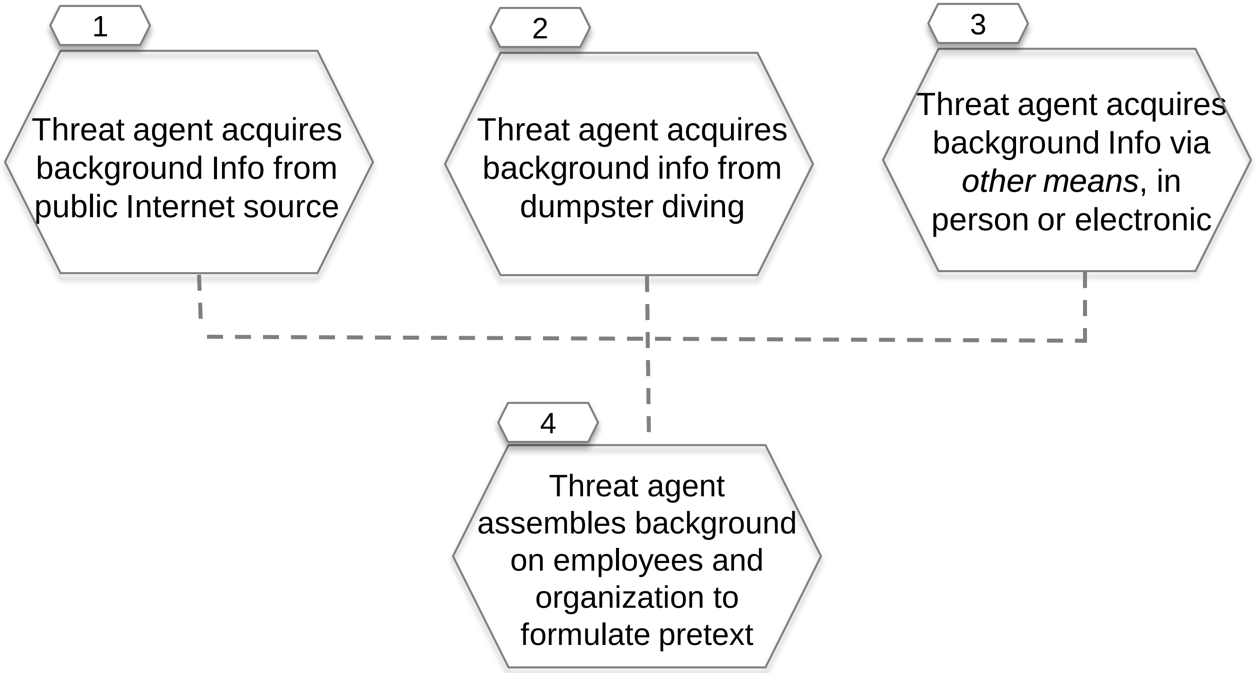
Description

A threat agent uses techniques of social engineering in order to persuade a victim to perform a desired action that results in an outcome that benefits the threat agent. Common examples of actions are to disclose particular information or to install/execute software that collects information or harms the victim's IT environment.

Notes

- The attack tree provides an overview of the use of social engineering, there are many varieties
- More details and common examples may be found at: http://www.social-engineer.org/framework/Social_Engineering_Framework

Common Tree: Threat Agent Uses Social Engineering <desired outcome> (1/2)



1

Threat agent acquires background Info from public Internet source

2

Threat agent acquires background info from dumpster diving

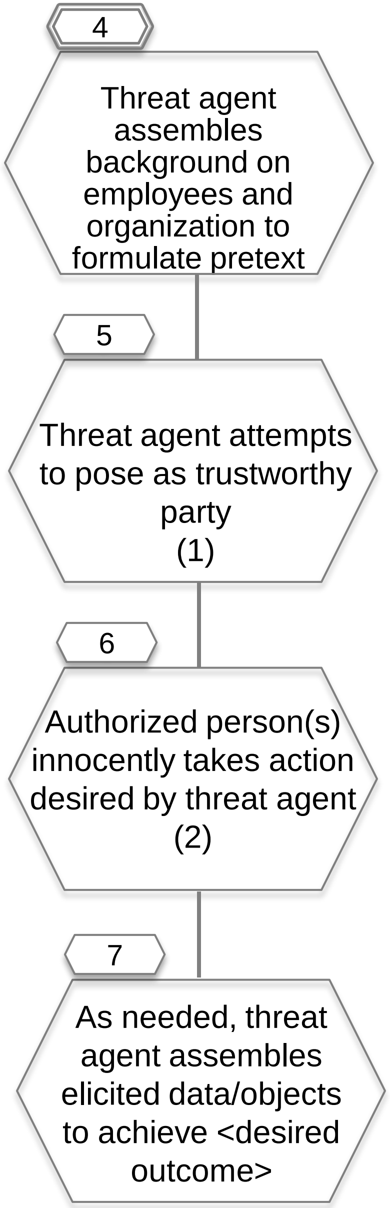
3

Threat agent acquires background Info via *other means*, in person or electronic

4

Threat agent assembles background on employees and organization to formulate pretext

Common Tree: Threat Agent Uses Social Engineering <desired outcome> (2/2)


4
Threat agent assembles background on employees and organization to formulate pretext
5
Threat agent attempts to pose as trustworthy party
(1)
6
Authorized person(s) innocently takes action desired by threat agent
(2)
7
As needed, threat agent assembles elicited data/objects to achieve <desired outcome>

(1) There are many effective techniques, all of which play on social/psychological aspects of trust. These can be pursued via any communication channel: in person (verbal/non-verbal), on the phone, email, voice mail, fax, postal mail.

(2) This can be to release sensitive data (e.g., via voice, digital message or on a web site) or release an object (such as key card), and/or to take some action that installs or executes a malicious program to gather data or performs other malicious actions.

Common Tree: Threat Agent Uses Social Engineering <desired outcome>

Potential Mitigations

1 - *Define policy* to minimize background internet disclosure, e.g. “do not make calendars public”

1,2,3,5,6 - *Conduct penetration testing* periodically, posing as a threat agent

2 - *Define policy* to minimize leakage of physical artifacts (e.g. shredding, locked receptacle)

5 - *Train personnel* that they are potentially targeted for these types of attacks and consequences for the organization can be serious.

5 - *Train personnel* to report social engineering attacks

5 - Track social engineering attacks and warn personnel

6 - *Train personnel* including users and administrators in procedures to foil threat agent e.g. “always call back to the number in the directory” and “always type in an authoritative web address”

Common Tree: Threat Agent Uses Social Engineering <desired outcome>

Potential Mitigations (2)

6 - *Detect abnormal behavior or functionality* via technical means, e.g. audit outgoing communications for sensitive data or unusual destinations

6 - *Authenticate messages* automatically, e.g. require digital signatures, cryptography on email to authenticate trustworthy parties

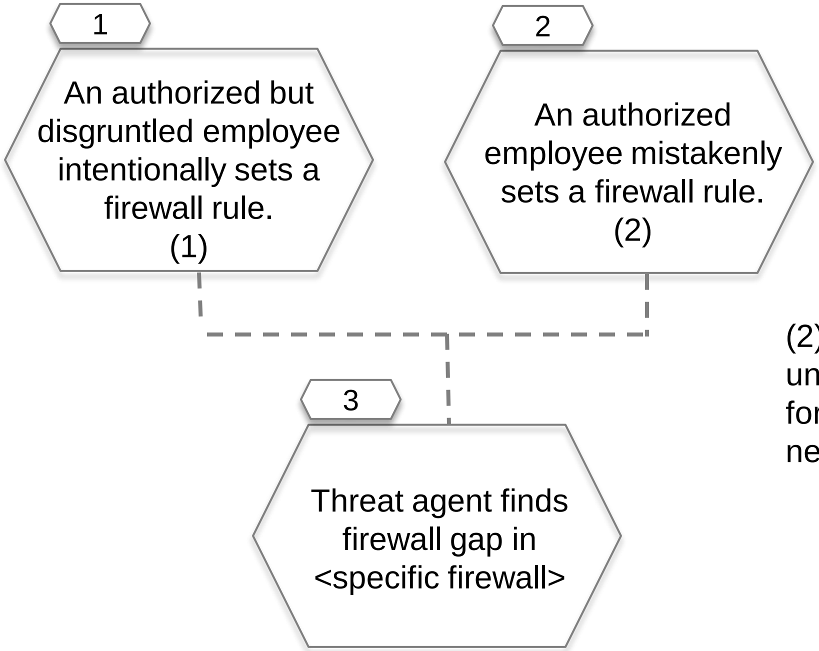
Common Tree: Threat Agent Finds Firewall Gap <specific firewall>

Description

An authorized employee either accidently or intentionally sets a firewall rule that allows an unnecessary and exploitable form of access to a network from another network.

Common Tree: Threat Agent Finds Firewall Gap <specific firewall>

(1) This rule allows an unnecessary and exploitable form of access between two networks



1

An authorized but disgruntled employee intentionally sets a firewall rule. (1)

2

An authorized employee mistakenly sets a firewall rule. (2)

3

Threat agent finds firewall gap in <specific firewall>

(2) This rule allows an unnecessary and exploitable form of access between two networks

Common Tree: Threat Agent Finds Firewall Gap <specific firewall>

Potential Mitigations

1, 2 - *Conduct penetration testing* to uncover firewall gaps, robust change/configuration management to protect entire system

1, 2 - *Implement configuration management* to reduce the likelihood that a threat agent can compromise an entire system

2 - *Verify* all firewall changes

3 - *Require intrusion detection and prevention*,

3 - *Require authentication* to network

3 - *Authenticate users* for firewall application and database access, logging, and monitoring,

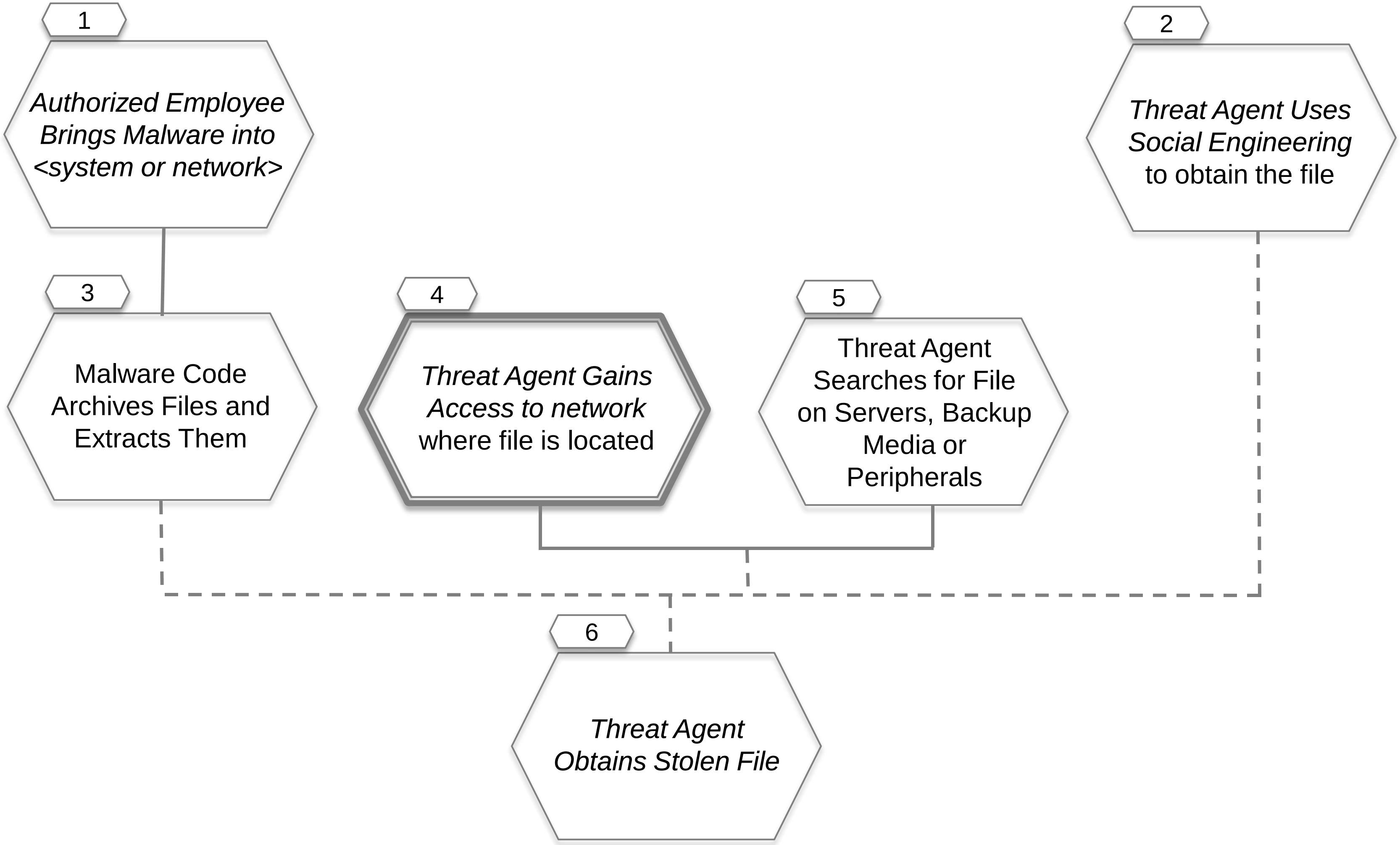
3 - *Restrict database access* for the firewall to authorized applications and/or locally authenticated users

Common Tree: Threat Agent Steals <file>

Description

A threat agent may use direct or indirect methods to obtain a copy of a file, including a direct break-in to the host holding the file, finding the file on back up media, scanning peripherals such as printers, and use of social engineering to influence a victim to give them the file.

Common Tree: Threat Agent Steals <file>



1

Authorized Employee Brings Malware into <system or network>

2

Threat Agent Uses Social Engineering to obtain the file

3

Malware Code Archives Files and Extracts Them

4

Threat Agent Gains Access to network where file is located

5

Threat Agent Searches for File on Servers, Backup Media or Peripherals

6

Threat Agent Obtains Stolen File

Common Tree: Threat Agent Steals <file>

Potential Mitigations

1 - *Train personnel* to protect against malware

1 - *Test for malware* on system or network

2 - See common tree *Threat Agent Uses Social Engineering* to obtain the file

3 - *Require on-going validation* of software/firmware

4 - See common tree *Threat Agent Gains Access* to network where file is located

5 - *Authenticate users* to servers, backup media, and peripherals

5 - *Detect unusual patterns* of usage on hosts and network

5 - *Enforce least privilege* for individuals with access to hosts on the network

6 - *Encrypt data at rest* for valuable files

Common Tree: Threat Agent Gains Access <network>

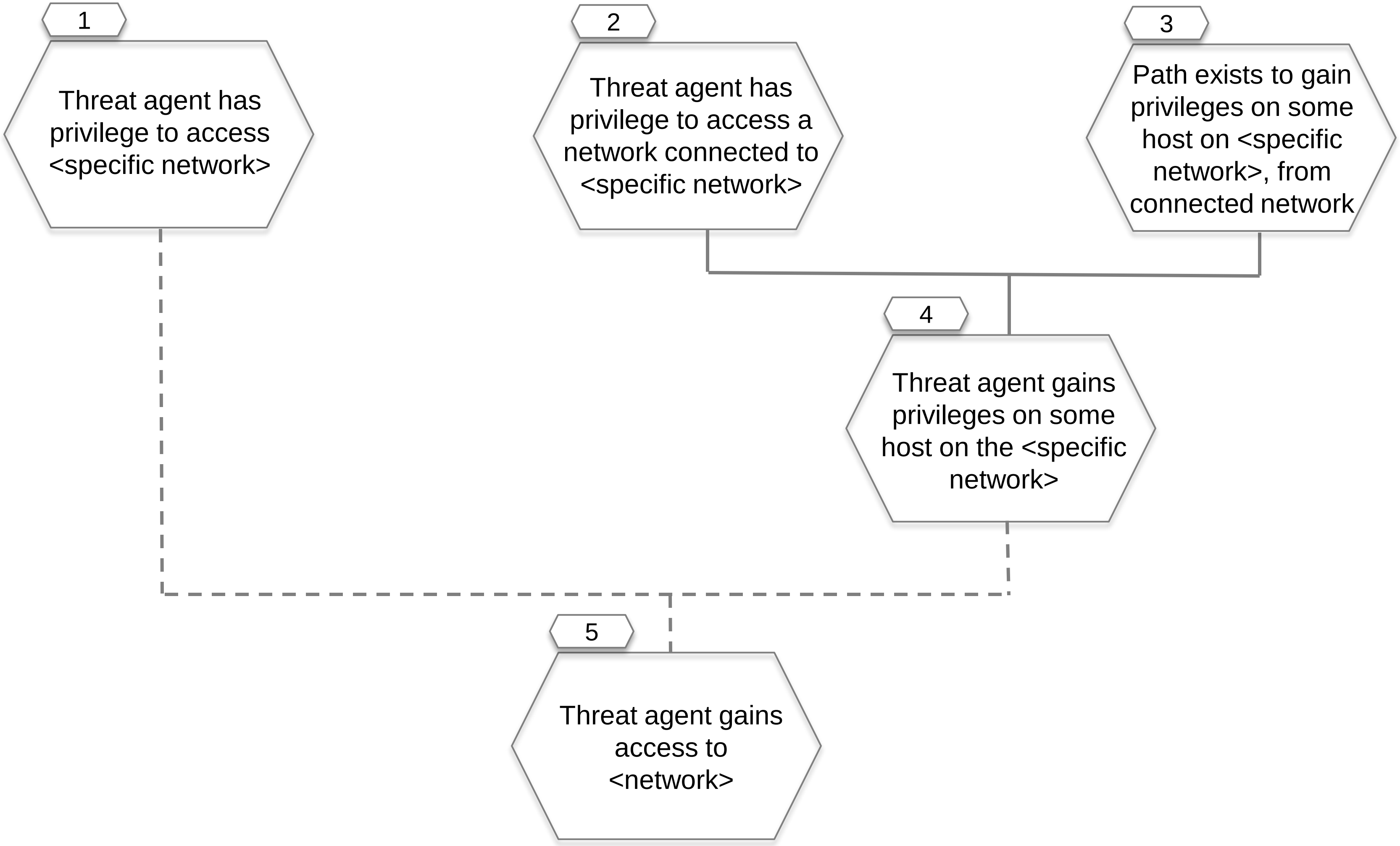
Description

A threat agent becomes capable of sending traffic within a network and attempting to communicate with its resident hosts.

Notes

- This draft tree currently expresses the high level concept of “bridging” sequentially between adjacent networks. Information should be added in future drafts related to:
  - Mitigations for detecting and preventing network reconnaissance
  - Specific differences in gaining access to networks that use various protocols and technologies

Common Tree: Threat Agent Gains Access <network>



1

Threat agent has privilege to access <specific network>

2

Threat agent has privilege to access a network connected to <specific network>

3

Path exists to gain privileges on some host on <specific network>, from connected network

4

Threat agent gains privileges on some host on the <specific network>

5

Threat agent gains access to <network>

Common Tree: Threat Agent Gains Access <network>

Potential Mitigations

1, 2 - *Enforce least privilege* to limit individuals with privilege to the network and connected networks

2 - *Isolate network*

3 - *Enforce restrictive firewall rules* for access to network

3 - *Design for security* by limiting connection points to networks that are widely accessible and by limiting number of hosts on same network

3 - *Require authentication* to the network

4 - *Enforce least privilege* for individuals with access to hosts on the network

5 - *Detect unusual patterns* of usage on hosts and network

Acronyms Used in Trees

AMI	Advanced Metering Infrastructure
AP	Access Point
DDOS	Distributed Denial of Service
DMS	Distribution Management System
DOS	Denial of Service
DR	Demand Response
DRAS	Demand Response Administration System
GUI	Graphical User Interface
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
MAC	Media Access Control
MITM	Man in the Middle

Acronyms Used in Trees (2)

NESCOR	National Electric Sector Cybersecurity Organization Resource
RBAC	Role Based Access Control
SCADA	Supervisory Control and Data Acquisition
S/W	Software
USB	Universal Serial Bus
3G	LTE Third Generation Long Term Evolution