Threat Modeling Report

Created on 24/03/2019 16:03:12

Threat Model Name: SiVES

Owner: Nivio Paula de Souza

Reviewer:

Contributors: Celso Massaki Hirata and Cecilia de Azevedo Castro Cesar

Description: Eletronic Voting System by Smartphone

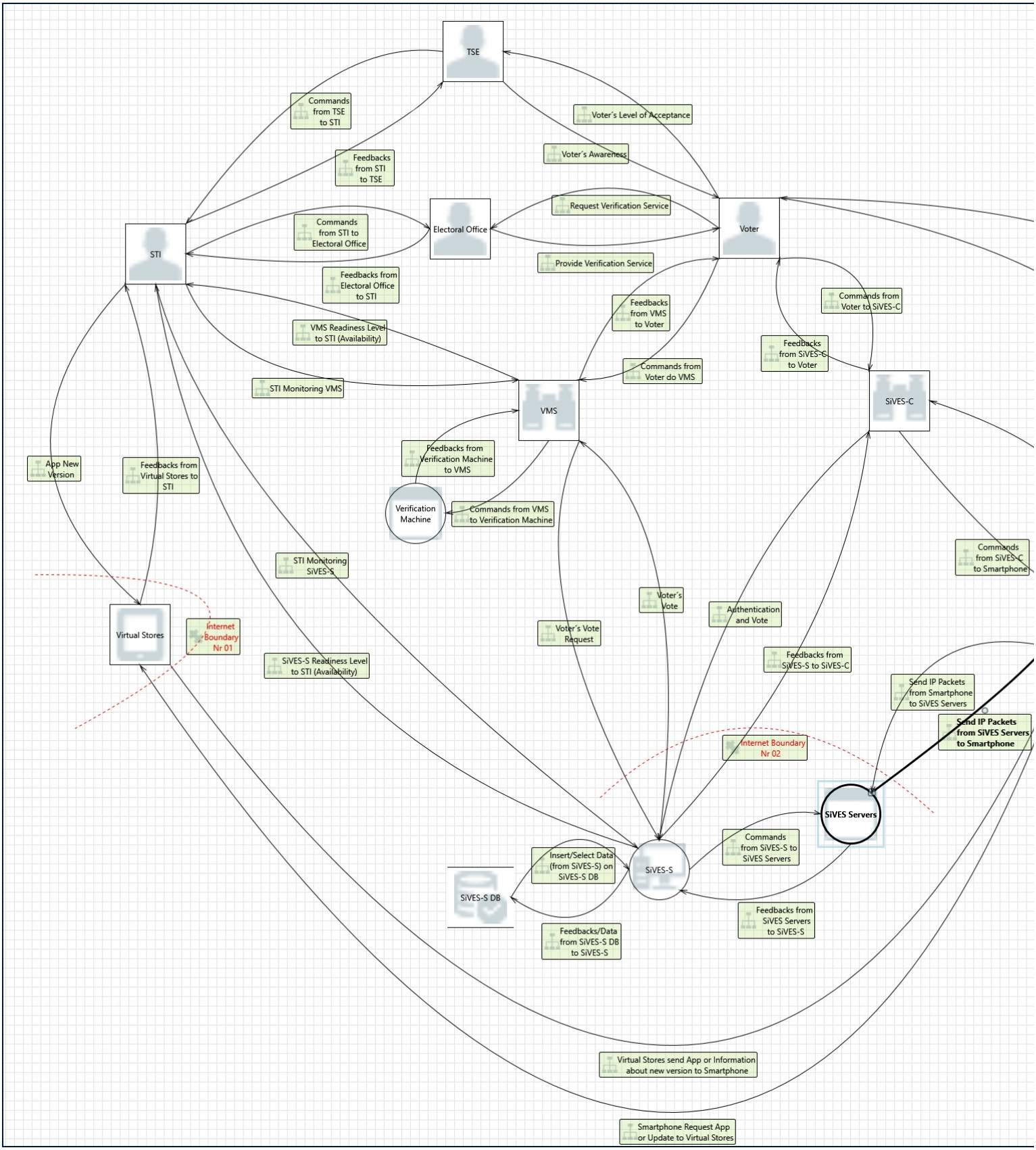
Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	0
Not Applicable	1
Needs Investigation	0
Mitigation Implemented	87
Total	88
Total Migrated	0

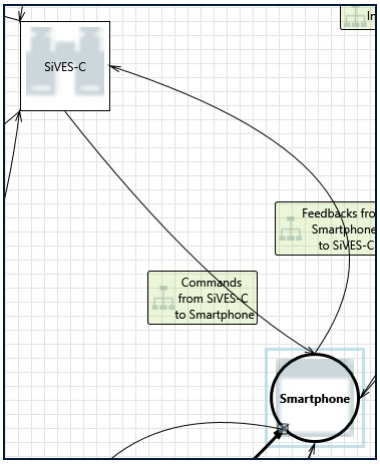
Diagram: Electronic Voting System by Smartphone



Electronic Voting System by Smartphone Diagram Summary:

Not Started	0
Not Applicable	1
Needs Investigation	0
Mitigation Implemented	87
Total	88
Total Migrated	0

Interaction: Commands from SiVES-C to Smartphone



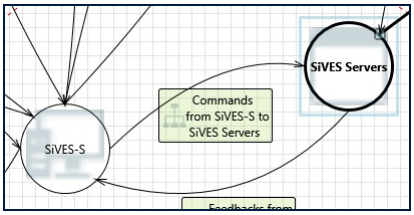
1. Spoofing the SiVES-C External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: SiVES-C may be spoofed by an attacker and this may lead to unauthorized access to Smartphone. Consider using a standard authentication mechanism to identify the external entity.
Justification: It is necessary to use authentication

2. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: Smartphone may be able to impersonate the context of SiVES-C in order to gain additional privilege.
Justification: It must be hardened and it is necessary to use authentication.

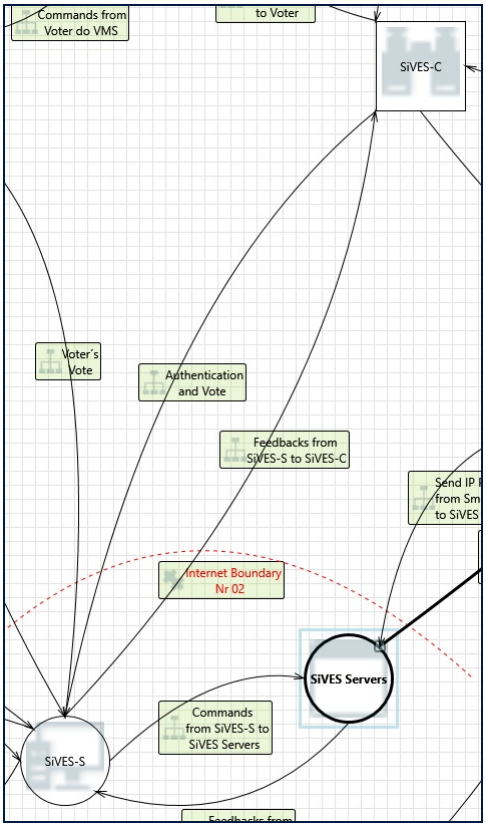
Interaction: Commands from SiVES-S to SiVES Servers



3. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: SiVES Servers may be able to impersonate the context of SiVES-S in order to gain additional privilege.
Justification: It must be hardened and it is necessary to use authentication.

Interaction: Feedbacks from SiVES-S to SiVES-C



4. Spoofing of the SiVES-C External Destination Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: SiVES-C may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of SiVES-C. Consider using a standard authentication mechanism to identify the external entity.

Justification: It is necessary to use authentication

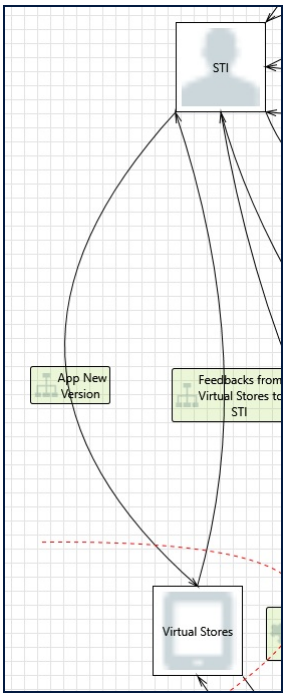
5. External Entity SiVES-C Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: SiVES-C claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification: Provide logs and auditing to ensure non-repudiation.

6. Data Flow Generic Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: The system must have means to avoid DoS attack, like redundancy.

Interaction: App New Version



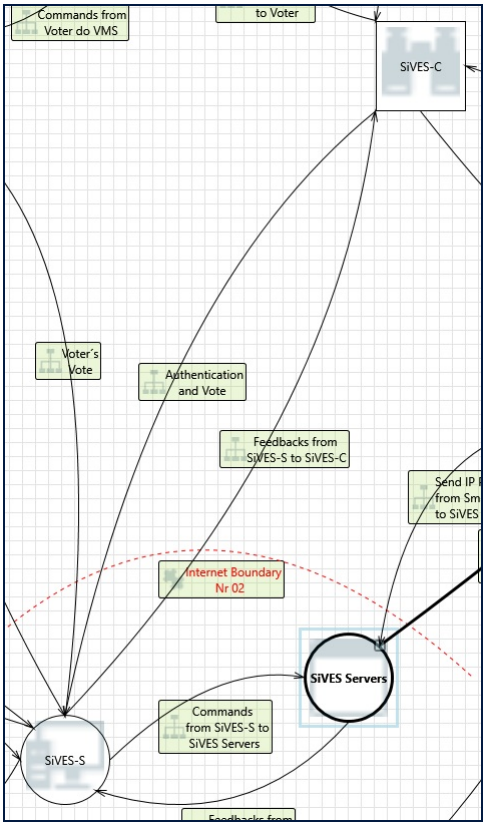
7. External Entity Virtual Stores Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: Virtual Stores claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification: Provide logs and auditing to ensure non-repudiation

8. Data Flow Generic Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: The system must have means to avoid DoS attack, like redundancy.

Interaction: Vote



9. Spoofing the SiVES-S Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: SiVES-S may be spoofed by an attacker and this may lead to information disclosure by SiVES-C. Consider using a standard authentication mechanism to identify the destination process.
Justification: It is necessary to use authentication

10. Spoofing the SiVES-C External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: SiVES-C may be spoofed by an attacker and this may lead to unauthorized access to SiVES-S. Consider using a standard authentication mechanism to identify the external entity.
Justification: It is necessary to use authentication

11. Potential Lack of Input Validation for SiVES-S [State: Mitigation Implemented] [Priority: High]

Category: Tampering
Description: Data flowing across Vote may be tampered with by an attacker. This may lead to a denial of service attack against SiVES-S or an elevation of privilege attack against SiVES-S or an information disclosure by SiVES-S. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.
Justification: All inputs must be validated before being used.

12. Cross Site Scripting [State: Mitigation Implemented] [Priority: High]

Category: Tampering
Description: The server 'SiVES-S' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.
Justification: All inputs must be validated before being used.

13. Potential Data Repudiation by SiVES-S [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: SiVES-S claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification: Provide logs and auditing to ensure non-repudiation.

14. Data Flow Sniffing [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure
Description: Data flowing across Vote may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.
Justification: It is necessary to use authentication and encrypted connections.

15. Potential Process Crash or Stop for SiVES-S [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: SiVES-S crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification: The system must be updated, setup correctly and have means to avoid DoS attack, like redundancy.

16. Data Flow Generic Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: The system must have means to avoid DoS attack, like redundancy.

17. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: SiVES-S may be able to impersonate the context of SiVES-C in order to gain additional privilege.
Justification: It must be hardened and it is necessary to use authentication.

18. SiVES-S May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: SiVES-C may be able to remotely execute code for SiVES-S.
Justification: It must be made system hardening, inputs validated and validate code to avoid exploitation.

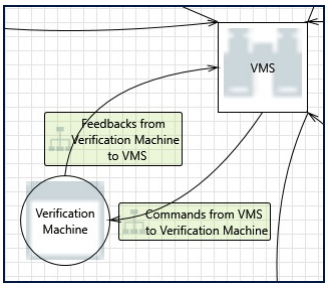
19. Elevation by Changing the Execution Flow in SiVES-S [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: An attacker may pass data into SiVES-S in order to change the flow of program execution within SiVES-S to the attacker's choosing.
Justification: It must be made system hardening, inputs validated and validate code to avoid exploitation.

20. Cross Site Request Forgery [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: Cross-site request forgery (CSRF or XSRF) is a type of attack in which an attacker forces a user's browser to make a forged request to a vulnerable site by exploiting an existing trust relationship between the browser and the vulnerable web site. In a simple scenario, a user is logged in to web site A using a cookie as a credential. The other browses to web site B. Web site B returns a page with a hidden form that posts to web site A. Since the browser will carry the user's cookie to web site A, web site B now can take any action on web site A, for example, adding an admin to an account. The attack can be used to exploit any requests that the browser automatically authenticates, e.g. by session cookie, integrated authentication, IP whitelisting, … The attack can be carried out in many ways such as by luring the victim to a site under control of the attacker, getting the user to click a link in a phishing email, or hacking a reputable web site that the victim will visit. The issue can only be resolved on the server side by requiring that all authenticated state-changing requests include an additional piece of secret payload (canary or CSRF token) which is known only to the legitimate web site and the browser and which is protected in transit through SSL/TLS. See the Forgery Protection property on the flow stencil for a list of mitigations.
Justification: It is necessary to harden system, use authentication and encrypted connections to avoid all these attacks.

Interaction: Commands from VMS to Verification Machine



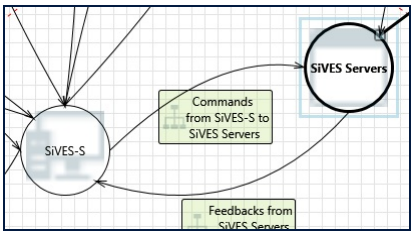
21. Spoofing the VMS External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: VMS may be spoofed by an attacker and this may lead to unauthorized access to Verification Machine. Consider using a standard authentication mechanism to identify the external entity.
Justification: It is necessary to use authentication

22. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: Verification Machine may be able to impersonate the context of VMS in order to gain additional privilege.
Justification: It must be hardened and it is necessary to use authentication.

Interaction: Feedbacks from SiVES Servers to SiVES-S



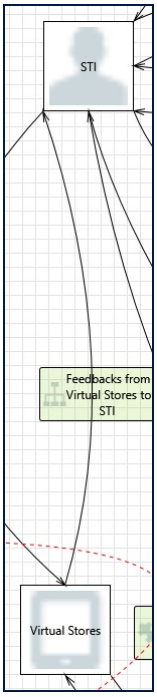
23. Cross Site Scripting [State: Mitigation Implemented] [Priority: High]

Category: Tampering
Description: The server 'SiVES-S' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.
Justification: All inputs must be validated before being used.

24. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: SiVES-S may be able to impersonate the context of SiVES Servers in order to gain additional privilege.
Justification: It must be hardened and it is necessary to use authentication.

Interaction: Feedbacks from Virtual Stores to STI



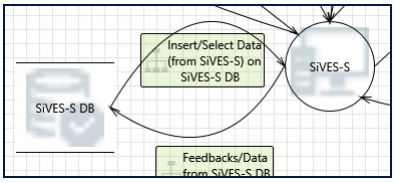
25. External Entity STI Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: STI claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification: Provide logs and auditing to ensure non-repudiation

26. Data Flow Generic Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: The system must have means to avoid DoS attack, like redundancy.

Interaction: Feedbacks/Data from SiVES-S DB to SiVES-S



27. Spoofing of Destination Data Store SQL Database [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: SiVES-S DB may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of SiVES-S DB. Consider using a standard authentication mechanism to identify the destination data store.
Justification: It is necessary to use authentication

28. Potential SQL Injection Vulnerability for SQL Database [State: Mitigation Implemented] [Priority: High]

Category: Tampering
Description: SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. Any procedure that constructs SQL statements should be reviewed for injection vulnerabilities because SQL Server will execute all syntactically valid queries that it receives. Even parameterized data can be manipulated by a skilled and determined attacker.
Justification: All inputs must be validated to prevent SQL injection or other exploitation of this way before being used.

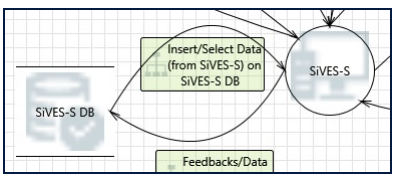
29. Potential Excessive Resource Consumption for SiVES-S or SQL Database [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: Does SiVES-S or SiVES-S DB take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.
Justification: It must controll resource consumption through anti DoS and DDoS tools (Akamai Network, etc.)

30. Weak Credential Storage [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure
Description: Credentials held at the server are often disclosed or tampered with and credentials stored on the client are often stolen. For server side, consider storing a salted hash of the credentials instead of storing the credentials themselves. If this is not possible due to business requirements, be sure to encrypt the credentials before storage, using an SDL-approved mechanism. For client side, if storing credentials is required, encrypt them and protect the data store in which they're stored
Justification: Credentials must be stored considering salted hash.

Interaction: Insert/Select Data (from SiVES-S) on SiVES-S DB



31. Spoofing of Source Data Store SQL Database [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: SiVES-S DB may be spoofed by an attacker and this may lead to incorrect data delivered to SiVES-S. Consider using a standard authentication mechanism to identify the source data store.
Justification: It is necessary to use authentication

32. Cross Site Scripting [State: Mitigation Implemented] [Priority: High]

Category: Tampering
Description: The server 'SiVES-S' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.
Justification: All inputs must be validated before being used.

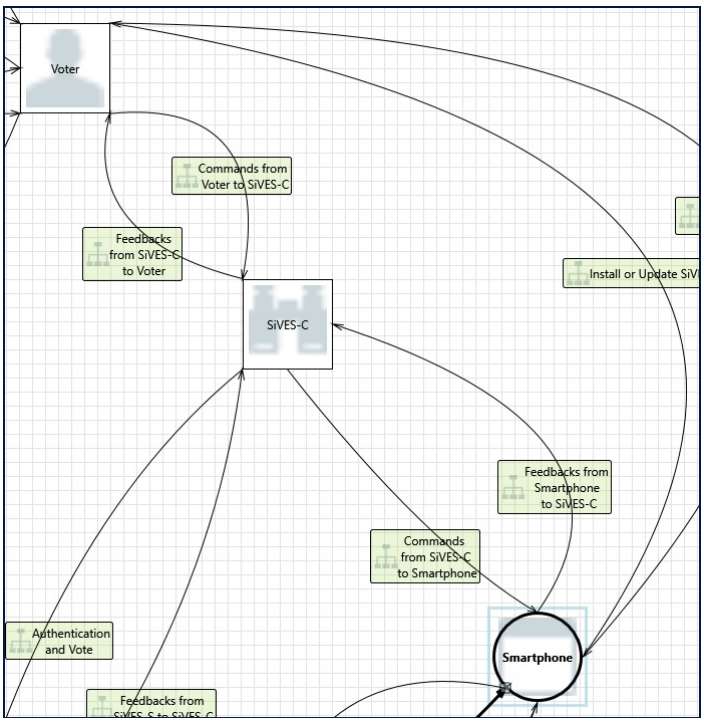
33. Persistent Cross Site Scripting [State: Mitigation Implemented] [Priority: High]

Category: Tampering
Description: The server 'SiVES-S' could be a subject to a persistent cross-site scripting attack because it does not sanitize data store 'SiVES-S DB' inputs and output.
Justification: All inputs must be validated before being used.

34. Weak Access Control for a Resource [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure
Description: Improper data protection of SiVES-S DB can allow an attacker to read information not intended for disclosure. Review authorization settings.
Justification: It must protect disclosure information by allowing access data only by predefined profiles.

Interaction: Install or Update SiVES-C



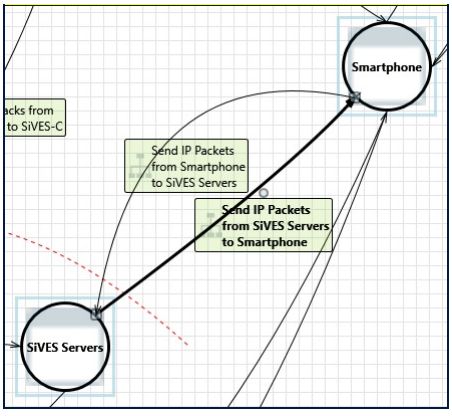
35. Elevation Using Impersonation [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege
Description: Smartphone may be able to impersonate the context of Voter in order to gain additional privilege.
Justification: <no mitigation provided>

36. Spoofing the Voter External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Voter may be spoofed by an attacker and this may lead to unauthorized access to Smartphone. Consider using a standard authentication mechanism to identify the external entity.
Justification: It is necessary to use authentication

Interaction: Send IP Packets from SiVES Servers to Smartphone



37. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: Smartphone may be able to impersonate the context of SiVES Servers in order to gain additional privilege.
Justification: It must be hardened and it is necessary to use authentication.

38. Spoofing the SiVES Servers Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: SiVES Servers may be spoofed by an attacker and this may lead to unauthorized access to Smartphone. Consider using a standard authentication mechanism to identify the source process.
Justification: It is necessary to use authentication

39. Spoofing the Smartphone Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Smartphone may be spoofed by an attacker and this may lead to information disclosure by SiVES Servers. Consider using a standard authentication mechanism to identify the destination process.
Justification: It is necessary to use authentication

40. Potential Data Repudiation by Smartphone [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: Smartphone claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification: Provide logs and auditing to ensure non-repudiation

41. Potential Process Crash or Stop for Smartphone [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: Smartphone crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification: The system must be updated, setup correctly and have means to avoid DoS attack, like redundancy.

42. Data Flow Send IP Packets from SiVES Servers to Smartphone Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: The system must have means to avoid DoS attack, like redundancy.

43. Smartphone May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: SiVES Servers may be able to remotely execute code for Smartphone.
Justification: It must be made system hardening, inputs validated and validate code to avoid exploitation.

44. Elevation by Changing the Execution Flow in Smartphone [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: An attacker may pass data into Smartphone in order to change the flow of program execution within Smartphone to the attacker's choosing.
Justification: It must be made system hardening, inputs validated and validate code to avoid exploitation.

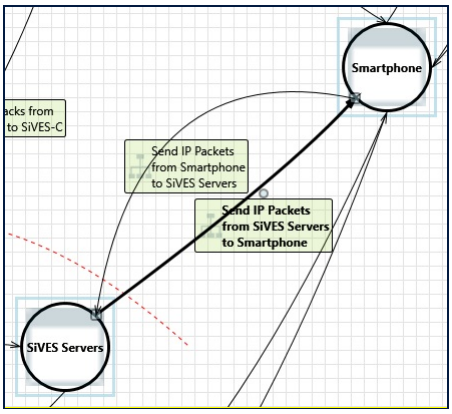
45. Potential Lack of Input Validation for Smartphone [State: Mitigation Implemented] [Priority: High]

Category: Tampering
Description: Data flowing across Send IP Packets from SiVES Servers to Smartphone may be tampered with by an attacker. This may lead to a denial of service attack against Smartphone or an elevation of privilege attack against Smartphone or an information disclosure by Smartphone. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.
Justification: All inputs must be validated before being used.

46. Data Flow Sniffing [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure
Description: Data flowing across Send IP Packets from SiVES Servers to Smartphone may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.
Justification: It is necessary to use authentication and encrypted connections.

Interaction: Send IP Packets from Smartphone to SiVES Servers



47. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: SiVES Servers may be able to impersonate the context of Smartphone in order to gain additional privilege.
Justification: It must be hardened and it is necessary to use authentication.

48. Spoofing the Smartphone Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Smartphone may be spoofed by an attacker and this may lead to unauthorized access to SiVES Servers. Consider using a standard authentication mechanism to identify the source process.
Justification: It is necessary to use authentication

49. Spoofing the SiVES Servers Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: SiVES Servers may be spoofed by an attacker and this may lead to information disclosure by Smartphone. Consider using a standard authentication mechanism to identify the destination process.
Justification: It is necessary to use authentication

50. Potential Data Repudiation by SiVES Servers [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: SiVES Servers claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification: Provide logs and auditing to ensure non-repudiation.

51. Potential Process Crash or Stop for SiVES Servers [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: SiVES Servers crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification: The system must be updated, setup correctly and have means to avoid DoS attack, like redundancy.

52. Data Flow Send IP Packets from Smartphone to SiVES Servers Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: The system must have means to avoid DoS attack, like redundancy.

53. SiVES Servers May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: Smartphone may be able to remotely execute code for SiVES Servers.
Justification: It must be made system hardening, inputs validated and validate code to avoid exploitation.

54. Elevation by Changing the Execution Flow in SiVES Servers [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: An attacker may pass data into SiVES Servers in order to change the flow of program execution within SiVES Servers to the attacker's choosing.
Justification: It must be made system hardening, inputs validated and validate code to avoid exploitation.

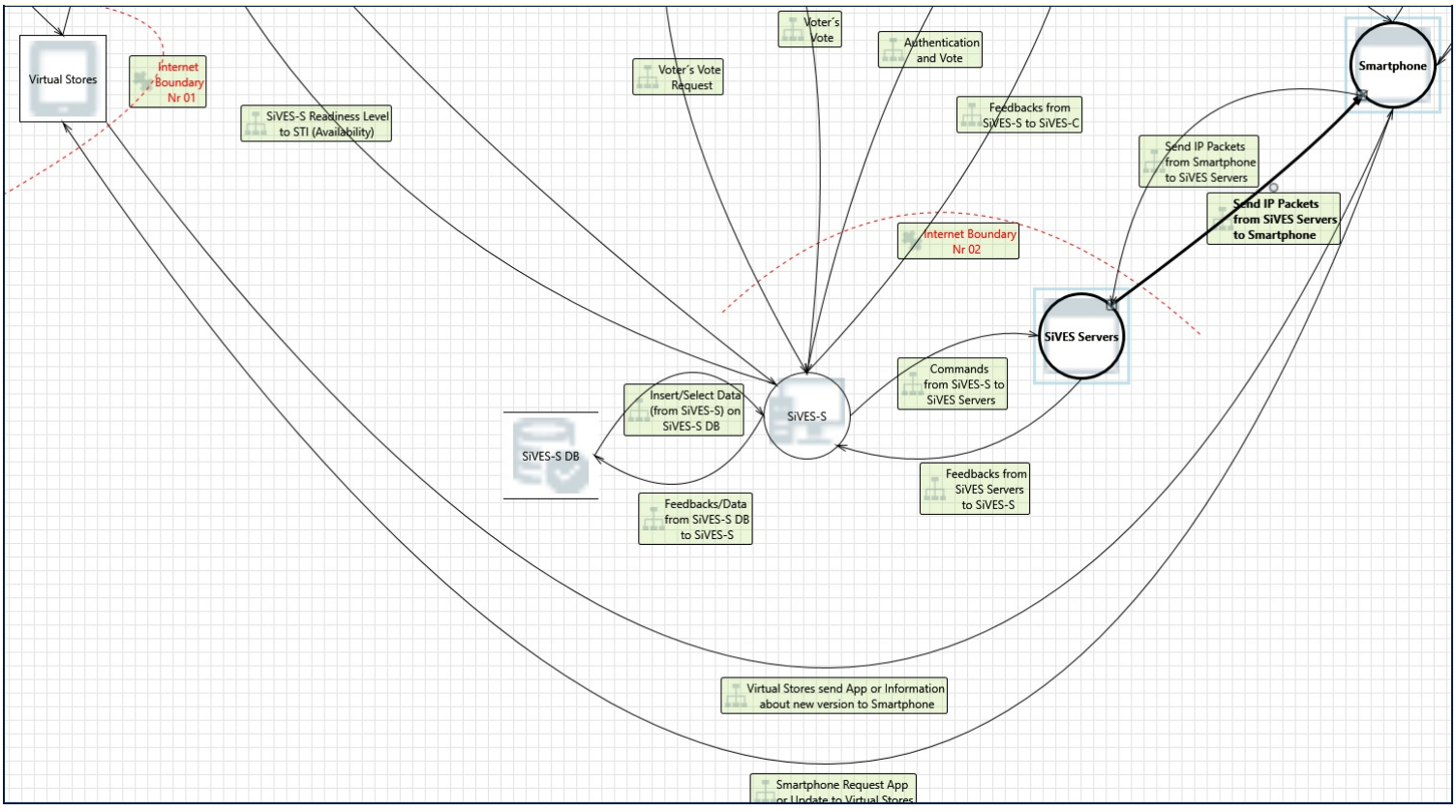
55. Potential Lack of Input Validation for SiVES Servers [State: Mitigation Implemented] [Priority: High]

Category: Tampering
Description: Data flowing across Send IP Packets from Smartphone to SiVES Servers may be tampered with by an attacker. This may lead to a denial of service attack against SiVES Servers or an elevation of privilege attack against SiVES Servers or an information disclosure by SiVES Servers. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.
Justification: All inputs must be validated before being used.

56. Data Flow Sniffing [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure
Description: Data flowing across Send IP Packets from Smartphone to SiVES Servers may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.
Justification: It is necessary to use authentication and encrypted connections.

Interaction: Smartphone Request App or Update to Virtual Stores



57. Data Flow Generic Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: The system must have means to avoid DoS attack, like redundancy.

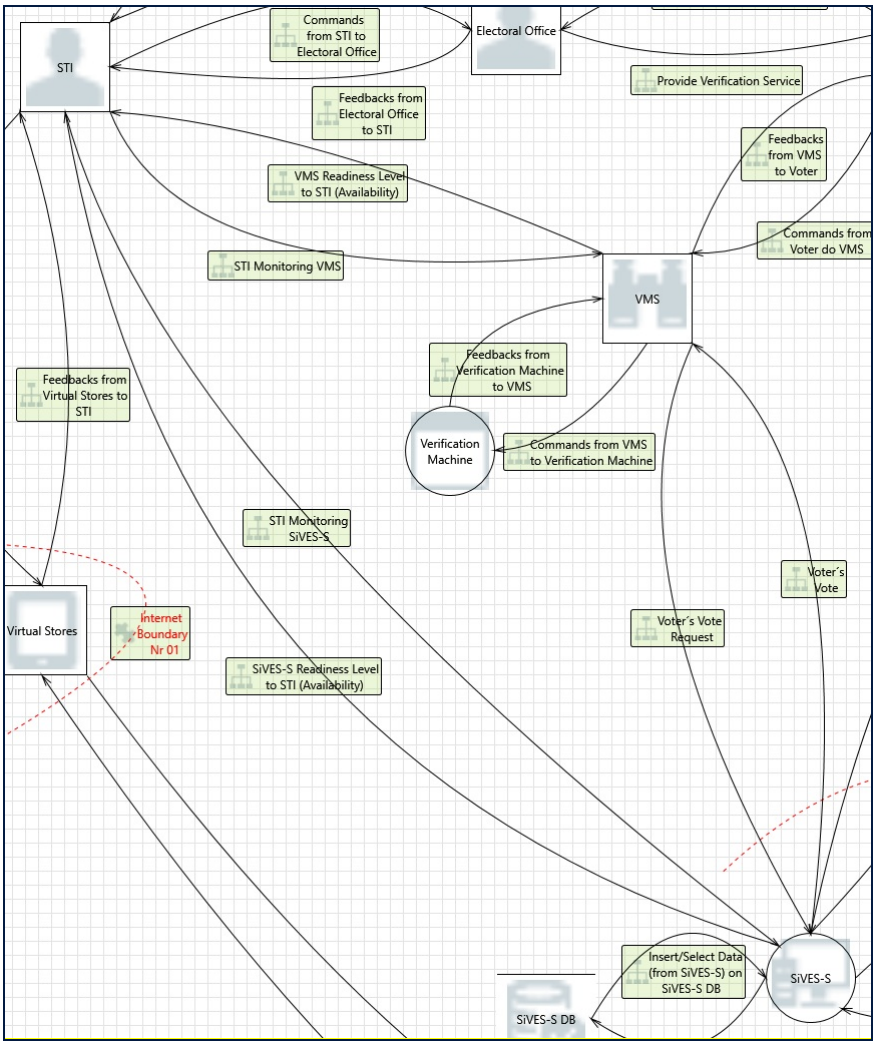
58. External Entity Virtual Stores Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: Virtual Stores claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification: Provide logs and auditing to ensure non-repudiation

59. Spoofing of the Virtual Stores External Destination Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Virtual Stores may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Virtual Stores. Consider using a standard authentication mechanism to identify the external entity.
Justification: It is necessary to use authentication

Interaction: STI Monitoring SiVES-S



60. Spoofing the STI External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: STI may be spoofed by an attacker and this may lead to unauthorized access to SiVES-S. Consider using a standard authentication mechanism to identify the external entity.
Justification: It is necessary to use authentication

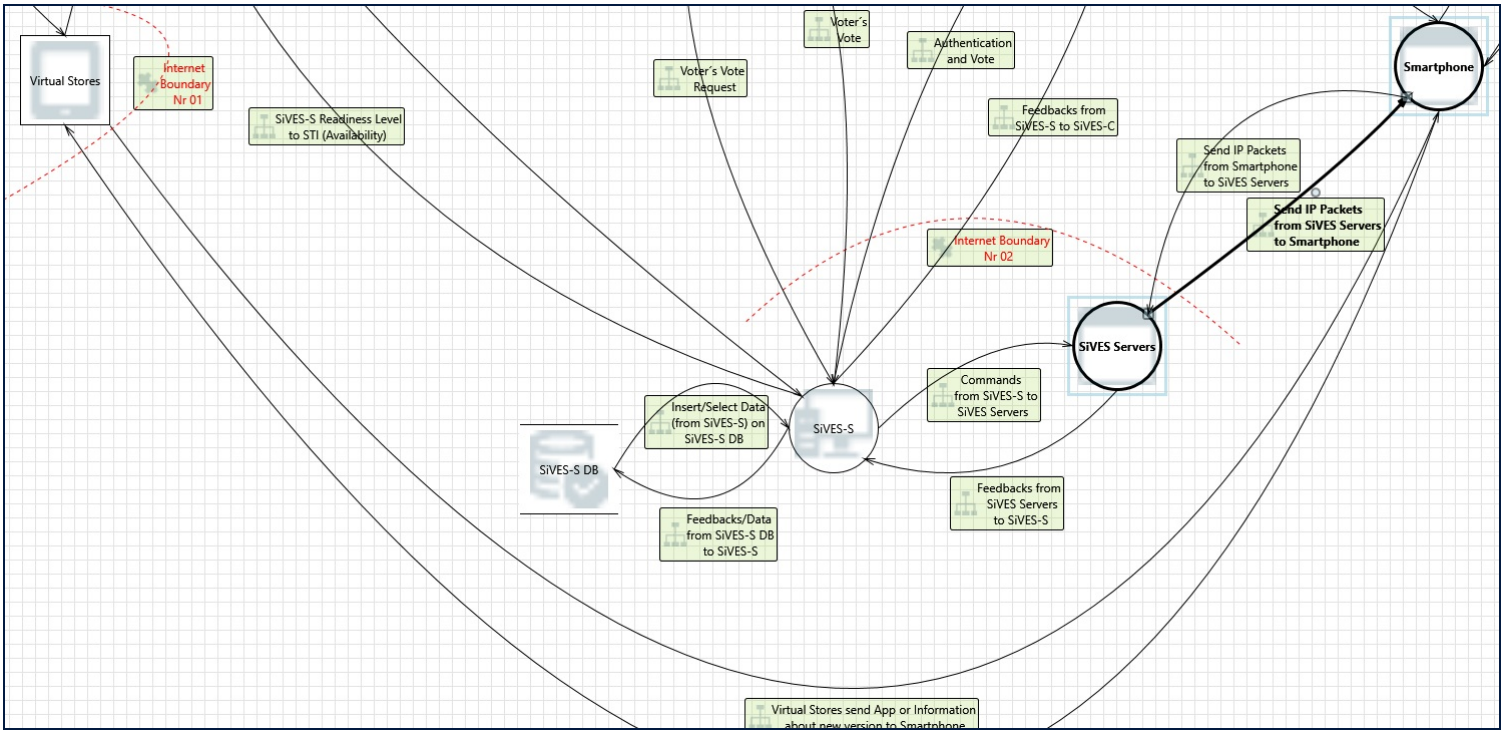
61. Cross Site Scripting [State: Mitigation Implemented] [Priority: High]

Category: Tampering
Description: The server 'SiVES-S' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.
Justification: All inputs must be validated before being used.

62. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: SiVES-S may be able to impersonate the context of STI in order to gain additional privilege.
Justification: It must be hardened and it is necessary to use authentication.

Interaction: Virtual Stores send App or Information about new version to Smartphone



63. Elevation by Changing the Execution Flow in Smartphone [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: An attacker may pass data into Smartphone in order to change the flow of program execution within Smartphone to the attacker's choosing.
Justification: It must be made system hardening, inputs validated and validate code to avoid exploitation.

64. Smartphone May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: Virtual Stores may be able to remotely execute code for Smartphone.
Justification: It must be made system hardening, inputs validated and validate code to avoid exploitation.

65. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: Smartphone may be able to impersonate the context of Virtual Stores in order to gain additional privilege.
Justification: It must be hardened and it is necessary to use authentication.

66. Data Flow Generic Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: The system must have means to avoid DoS attack, like redundancy.

67. Potential Process Crash or Stop for Smartphone [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: Smartphone crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification: The system must be updated, setup correctly and have means to avoid DoS attack, like redundancy.

68. Data Flow Sniffing [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure
Description: Data flowing across Virtual Stores send App or Information about new version to Smartphone may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.
Justification: It is necessary to use authentication and encrypted connections.

69. Potential Data Repudiation by Smartphone [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: Smartphone claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification: Provide logs and auditing to ensure non-repudiation

70. Potential Lack of Input Validation for Smartphone [State: Mitigation Implemented] [Priority: High]

Category: Tampering
Description: Data flowing across Virtual Stores send App or Information about new version to Smartphone may be tampered with by an attacker. This may lead to a denial of service attack against Smartphone or an elevation of privilege attack against Smartphone or an information disclosure by Smartphone. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.
Justification: It is necessary to use authentication, encrypted connections (with hash algorithm) and to have means to avoid DoS attack, like redundancy.

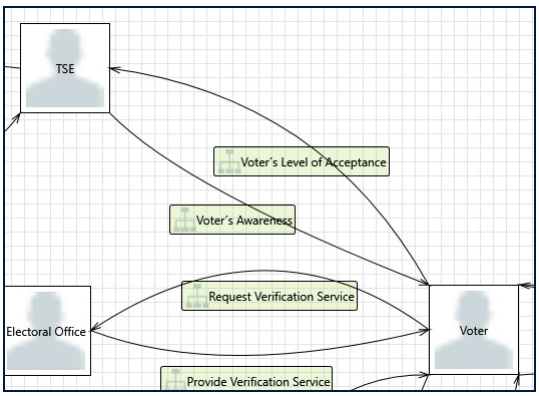
71. Spoofing the Virtual Stores External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Virtual Stores may be spoofed by an attacker and this may lead to unauthorized access to Smartphone. Consider using a standard authentication mechanism to identify the external entity.
Justification: It is necessary to use authentication

72. Spoofing the Smartphone Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Smartphone may be spoofed by an attacker and this may lead to information disclosure by Virtual Stores. Consider using a standard authentication mechanism to identify the destination process.
Justification: It is necessary to use authentication

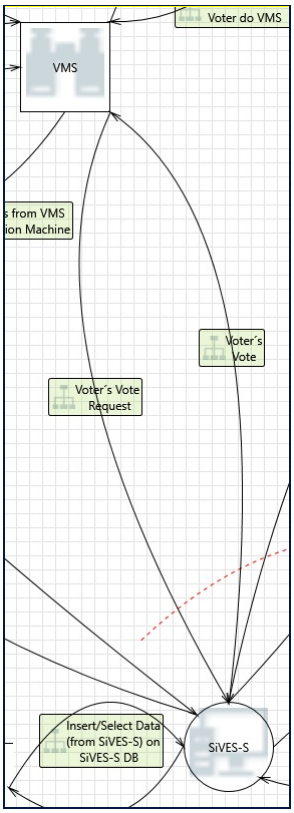
Interaction: Voter´s Level of Acceptance



73. Authenticated Data Flow Compromised [State: Mitigation Implemented] [Priority: High]

Category: Tampering
Description: An attacker can read or modify data transmitted over an authenticated dataflow.
Justification: It is necessary to use encrypted connections (with hash algorithm) to ensure confidentiality and data integrity.

Interaction: Voter´s Vote Request



74. Spoofing the SiVES-S Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: SiVES-S may be spoofed by an attacker and this may lead to information disclosure by VMS. Consider using a standard authentication mechanism to identify the destination process.
Justification: It is necessary to use authentication

75. Spoofing the VMS External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: VMS may be spoofed by an attacker and this may lead to unauthorized access to SiVES-S. Consider using a standard authentication mechanism to identify the external entity.
Justification: It is necessary to use authentication

76. Potential Lack of Input Validation for SiVES-S [State: Mitigation Implemented] [Priority: High]

Category: Tampering
Description: Data flowing across Voter´s Vote Request may be tampered with by an attacker. This may lead to a denial of service attack against SiVES-S or an elevation of privilege attack against SiVES-S or an information disclosure by SiVES-S. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.
Justification: All inputs must be validated before being used.

77. Cross Site Scripting [State: Mitigation Implemented] [Priority: High]

Category: Tampering
Description: The server 'SiVES-S' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.
Justification: All inputs must be validated before being used.

78. Potential Data Repudiation by SiVES-S [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: SiVES-S claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification: Provide logs and auditing to ensure non-repudiation.

79. Data Flow Sniffing [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure
Description: Data flowing across Voter´s Vote Request may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.
Justification: It is necessary to use authentication and encrypted connections.

80. Potential Process Crash or Stop for SiVES-S [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: SiVES-S crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification: The system must be updated, setup correctly and have means to avoid DoS attack, like redundancy.

81. Data Flow Generic Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: The system must have means to avoid DoS attack, like redundancy.

82. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: SiVES-S may be able to impersonate the context of VMS in order to gain additional privilege.
Justification: It must be hardened and it is necessary to use authentication.

83. SiVES-S May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: VMS may be able to remotely execute code for SiVES-S.
Justification: It must be made system hardening, inputs validated and validate code to avoid exploitation.

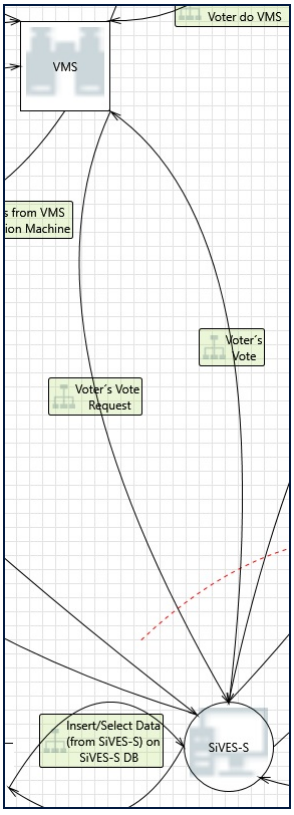
84. Elevation by Changing the Execution Flow in SiVES-S [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: An attacker may pass data into SiVES-S in order to change the flow of program execution within SiVES-S to the attacker's choosing.
Justification: It must be made system hardening, inputs validated and validate code to avoid exploitation.

85. Cross Site Request Forgery [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: Cross-site request forgery (CSRF or XSRF) is a type of attack in which an attacker forces a user's browser to make a forged request to a vulnerable site by exploiting an existing trust relationship between the browser and the vulnerable web site. In a simple scenario, a user is logged in to web site A using a cookie as a credential. The other browses to web site B. Web site B returns a page with a hidden form that posts to web site A. Since the browser will carry the user's cookie to web site A, web site B now can take any action on web site A, for example, adding an admin to an account. The attack can be used to exploit any requests that the browser automatically authenticates, e.g. by session cookie, integrated authentication, IP whitelisting, … The attack can be carried out in many ways such as by luring the victim to a site under control of the attacker, getting the user to click a link in a phishing email, or hacking a reputable web site that the victim will visit. The issue can only be resolved on the server side by requiring that all authenticated state-changing requests include an additional piece of secret payload (canary or CSRF token) which is known only to the legitimate web site and the browser and which is protected in transit through SSL/TLS. See the Forgery Protection property on the flow stencil for a list of mitigations.
Justification: It is necessary to harden system, use authentication and encrypted connections to avoid all these attacks.

Interaction: Voter´s Vote



86. Spoofing of the VMS External Destination Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: VMS may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of VMS. Consider using a standard authentication mechanism to identify the external entity.
Justification: It is necessary to use authentication

87. External Entity VMS Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: VMS claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification: Provide logs and auditing to ensure non-repudiation.

88. Data Flow Generic Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: The system must have means to avoid DoS attack, like redundancy.