2019 STAMP Workshop
March, 25-28, 2019, MIT, Cambridge

http://sunnyday.mit.edu/

USING STAMP FOR ANALYSIS OF SECURITY AND DATA PRIVACY

Nívio P. Souza, ITA

Cecília A. C. Cesar, ITA

Juliana M. Bezerra, ITA

Celso M. **Hirata**, ITA- **hirata@ita.br**

Disclaimer

The considerations herein expressed are of the authors of this presentation and do not reflect the official position of the Tribunal Superior Eleitoral do Brasil or the Brazilian Government.

Agenda

- Motivation
- Goal
- Some Background
- Using STAMP for safety, security, and privacy: a Proposal
- SiVES: System of e-Voting using Smartphone
  - Results and Analysis
- Conclusions

Motivation

- More complex systems, factors not only technical but also sociological, political and legal
- Cyber Security is a **strategic concern** for many businesses.
- Privacy gaining attention due to the **increasing legal protection of the right to data privacy**.
- STAMP allows analyzing emergent properties in the **concept stage**.
  - Safety (STPA) and, more recently, security (STPA-Sec).

- How to consider security and **privacy** in STAMP?

Goal

- Propose an approach that allows analyzing safety, security and privacy of systems using STAMP/STPA-Sec in order to identify hazardous control actions and generate requirements.
- The approach employs guidelines to consider data privacy, safety and security.
- We use as an example the Brazilian electronic voting system to vote using smartphones.

Some Background

- STAMP and STPA-Sec (Monday sessions)
- Some more Security
- Data Privacy

Security

- Security - concurrent existence of **availability, confidentiality, and integrity**.
- Availability - **readiness for correct service**.
- Confidentiality - **absence of unauthorized disclosure of information**.
- Integrity - **absence of non-authorized system alterations**.
- Security analysis techniques allow eliciting security requirements by considering assets, vulnerabilities, **threats**, and risks.
- Techniques usually employed in the Design Phase.

Security

- In an online banking site, clients require **confidentiality of the transaction**, **integrity of the data**, and **service availability in accessing** the online banking site.
- Security of the access to the online banking is determined by technological mechanisms.
- Mechanisms include computer access control, antivirus software, authentication, authorization, encryption, firewall, and intrusion detection system.
- Security Threat models, such as STRIDE (Microsoft), can be used to identify requirements.
- **Spoofing of user identity, Tampering, Repudiation, Information disclosure (privacy breach or data leak), Denial of service (DoS), Elevation of privilege.**
- Threat models are seen as more effective to analyze security and generate requirements because they consider wider spectrum of causes.

Data Privacy

- Privacy: **need** of conceptualization - **legal and policy decisions**
- **"the right to informational self-determination", allowing individuals to "control, edit, manage, and delete information about themselves and decide when, how, and to what extent that information is communicated to others" [Hansen, 2008]**
- **Data protection** - protecting any information relating to a person, such as name and address.
  - Stems from the right to privacy - instrumental to exercise other rights and freedoms.
- Data protection involves three entities**:**
- **data subject** -identifiable individual to whom personal data relate)
- **data processor** - entity that processes personal information
- **data controller** - who **determines** the purposes for which and the manner in which any item of personal information is processed.

Privacy attributes

- **Unlinkability** - hiding the link between two or more actions, identities, and pieces of information.
- **Anonymity** - hiding the link between an identity and an action or a piece of information.
- **Pseudonymity** - possible to build a plausible deniability reputation on a pseudonym.
- **Plausible deniability** – possible to deny having performed an action that other parties can neither confirm nor contradict.
- **Undetectability** - hiding the user's activities.
- **Confidentiality** - hiding the data content or controlled release of data content.
- **Content awareness** - user needs to be aware of the consequences of sharing information.
- **Consent compliance** requires the data controller to inform the data subject about the system's privacy policy, or allow the data subject to specify consents in compliance with legislation.
- [Deng, 2010]

Data privacy

- In an online drug store, clients require security and privacy to transact.
- Clients want to keep their information protected (identity, medical prescription, drug). They might consent to have their information shared (for the purpose of some discount program).
- **Clients do not want to be identified. They want to be able to repudiate any link with the transaction. They do not want to have their information disclosed (even the access to the site). They want to know about the consent that they are providing and the privacy policy of the store.**
- In general, the security and privacy requirements are met by the same technological mechanisms. Privacy require some additional mechanisms.

Privacy Threat Model: LINDDUN

- Privacy Threat models, such as LINDDUN, can be used to identify requirements.
- Each letter of "LINDDUN" stands for a privacy threat type obtained by negating a privacy property, indicating a privacy threat category. There is almost one-to-one correspondence between threats and attributes.
- **L**inkability of two or more items of interest, **I**dentifiability of a subject (*anonymity*, *pseudonymity*), **N**on-repudiation, **D**etectability of an item of interest, Information **D**isclosure, Content **U**nawareness, and Policy and Consent **N**on-compliance.

Using STAMP for safety, security, and privacy: a Proposal

- STAMP models tasks: Define system mission, purpose, goal, and key activities, **Identify unacceptable losses (accidents) and hazards/constraints,** Model the functional control structure, and Check Functional Control Structure Model for completeness.
- We propose an extension to the task Identify unacceptable losses and hazards/ constraints.
  - Characterization of Unacceptable Losses in terms of Security and Privacy
  - Characterization of Hazards in terms of Security and Privacy

Characterization of Unacceptable Losses in terms of Security and Privacy

- Loss refers to **compensating cost, loss of credibility** in a service or institution, political damages, and so on, due to a security breach, lack of security, privacy violation or lack of privacy.
- Unacceptable loss in terms of occurrence of an unwanted event, its number or frequency, and its severity.
  - For some systems, a single occurrence of an event is unacceptable.
  - The frequency and severity of events can be dealt either quantitatively or qualitatively. The qualification, quantification, and the act of unacceptance are made by responsible stakeholders.
  - Frequency is measured over a period of time. The frequency of service events must be monitored.

Characterization of Unacceptable Losses in terms of Security

- Unacceptable loss can be the characterized as a combination of the violations of security attributes or realizations of security threats.
  - **Loss of credibility due to unacceptable number and severity of security issues.**
- We can use security attributes to characterize a loss.
  - **Loss of reputation due to a large number of violations of confidentiality**.
- We can use threats. STRIDE is an acronym for Spoofing, Tampering, Repudiation, Information Disclosure, **Denial of Service**, and Elevation of Privilege.
  - **Loss of revenue due to successful Denial of Service attacks.**

Characterization of Unacceptable Losses in terms of Privacy using Attribute

- **The idea is to use privacy attributes or privacy threats.**
- Loss of credibility due to violation of privacy loss due to any occurrence of linkability that links a voter to a vote

Characterizing Hazards in terms of Security and Privacy

- For physical systems, hazard is associated to some physical condition, for instance, distance between two aircrafts.
- Cyber physical systems may change states upon receiving and processing messages and reacting by sending messages (events).
- These events may not characterize any change of physical condition.
- **We propose to employ <u>state</u> that leads to the occurrence of security and privacy threats or violations of security and privacy attributes.**

Characterizing Hazards in terms of Security and Privacy

- In the voting system, for the unacceptable loss “Loss of credibility due to violation of privacy loss due to any occurrence of linkability that links a voter to a vote”, we identify two hazards:
  - State that allows information disclosure that links voter to vote (linkability). The state is characterized when the voting transaction is undisclosed.
  - State that does not allow a voter to deny for whom he/she voted. (Non-repudiation). The state is characterized when the following election report (after tallying the votes) is possible: “All the votes collected in an electoral area were given to one candidate”
- The challenge is to find these states. This requires thinking of states that lead to the unacceptable losses using attributes and threats to security and privacy.

SiVES: System of e-Voting using Smartphone

- We apply the characterizations of security and privacy in an example.
- STAMP models are constructed using the following descriptions: the system purpose, system description, unacceptable losses, hazards, and the functional control structure for safety, security and privacy analysis.
- **The purpose of the system is to allow voting of users using smartphones, meeting Electoral Higher Court guidelines, through the registration of biometric data's voters in the electoral office, system set up, call for voting, app installation, voting, tallying, and verification to contribute to the Brazilian democracy.**
- Key stakeholders are voters, Electoral Higher Court (known as TSE in Brazil), Information Technology Secretary (STI) and virtual stores (Apple Store and Google Play).

SiVES: Assumptions and Restrictions

- SiVES is a smartphone electronic voting system based on the assumptions and restrictions described as follows.
- The biometry is fingerprint and the enrollments of voters are already made.
- For voters, SiVES has three methods: application installation on smartphones, operation (voting), and verification of the vote. SiVES must allow the voter to vote and verify that the vote was correctly counted (verifiability).
- SiVES has the server component (SiVES-S) that runs on server computers in STI and the client component (SiVES-C) that runs in the voter's smartphone. The voting process allows ‘revoting’. The valid vote is the last one.
- SiVES is available to voters for a given period. Afterwards, only the in person voting is possible.
- SiVES must allow the voter to verify that the system has counted his/her vote correctly (verifiability). The verification occurs in verification machines inside electoral office.

SiVES Key Activities

- We focus on Operation. Development is not addressed here.
- In operation, we identify the following **key activities: registration of biometric data's voters in the electoral office, system set up, call for voting, app installation, voting, tallying (**it is considered for the control structure, but it is not analyzed), **and verification.**
- We do not consider the activity of registration of biometric data's voters in the electoral office for elaborating the functional control structure.

SiVES Key Activities

- **System set up** is about installing all the hardware and software, including the network, to run the server system. It also includes the upload of the installation package in the app stores by STI.
- **Call for voting** is the public call to all the voters. It is the responsibility of TSE.
- **Application installation** refers to installation of the app in the smartphone. Installation is the responsibility of voters.
- In **voting**, the voter authenticates herself/himself in the system and votes.
- In **tallying**, STI tallies the votes and TSE makes the results public. It is considered for the functional control structure, but it is not be analyzed here.
- In **verification,** the voter goes to the electoral office and checks his/her vote.
- We perform the analysis for system set up, call for voting, application installation, voting and verification - activities where the voters interact with the system.

SiVES: Unacceptable Losses

- We identify the following Unacceptable Security and Privacy Losses:

  UL1: Unacceptable number of eligible voters who are unable to vote

  UL2: Unacceptable number of eligible voters who are unable to verify the vote.

  UL3: Loss of credibility due to unacceptable number and severity of security issues.

  UL4: Loss of credibility due to violation of data privacy

- We assume that definitions of the numbers of eligible voters who are unable to vote and verify the vote are defined by a proper responsible role.

SiVES: Hazards

- We identify the following hazards:

H1: Voters unable to vote due to reliability, availability and mission assurance issues. (UL1)

H1.1: State that does not allow a legitimate voter to vote (to assure the mission).

H1.2: State that prevents voting due to the system's unavailability and reliability issues.

H2: Voters unable to verify the vote (reliability, availability and mission assurance issues). (UL2)

H2.1: State that does not allow a legitimate voter who voted to verify his/her own vote (to assure the mission).

H2.2: State that prevents to verify the vote due to the system's unavailability and reliability issues.

SiVES: Hazards

- We identify the following hazards:

H3: State that allows security violations (security issues). (UL3)

H3.1: State that allows unauthorized access to private information (data, vote, etc.).

H3.2: State that allows an unauthorized person to vote.

H3.3: State that allows for undue alteration of the voter's vote.

H4: State that allows data privacy loss (privacy issues) (UL4)

H4.1: State that allows information disclosure that links voter to a vote.

H4.2: State that does not allow a voter to deny to whom he/she voted for.

SiVES: Functional Control Structure

- Using the key activities (registration of biometric data’s voters, system set up, call for voting, app installation, voting, tallying, and verification) to **identify model elements.**
- **Identify responsibilities of model elements** in carrying out each of the key activities necessary to conduct the mission.
- **Identify control relationships**.
- For each controller element
  - **Identify control actions** necessary to execute its responsibilities
  - Develop description of the process model
    - **Identify the process model variables**
    - For each variable, **identify the values** and the feedback or communication link

SiVES: Identify Model Elements

Method (Key activity)	Model Elements	Description
System set up, call for voting and application installation	TSE, STI, Virtual Stores, Voter, Smartphone	Elements that have responsibilities in the system set up, call for voting and application installation
Voting	**STI, SiVES-S, SiVES Servers, SiVES-C, Voter**	**Elements that have responsibilities in the voting**
Tallying	TSE, STI, SiVES-S	Elements that have responsibilities in the tallying
Verification	STI, Electoral Zone, Verification Machine, Verification Machine Software (VMS), SiVES-S, SiVES Servers , Voter	Elements that have responsibilities in the verification

SiVES: Identify responsibilities of model elements for **Voting**.

Model Element	Responsibility for "Voting"
STI	- Make SiVES-S available to voting method
Voter	- Follow security and privacy TSE guidelines - Authenticate - Accept the privacy agreement - Vote
SiVES-C	- Capture biometric data for SiVES-C - Send request of authentication to SiVES-S - Present result of the authentication - Offer privacy agreement - Send the acceptance of the privacy agreement to SiVES-S - Send the vote - Present voting confirmation or error
SiVES-S	- Provide authentication - Send result of the authentication - Register the acceptance of the privacy agreement - Register the vote sent by SiVES-C - Send the voting confirmation or error

SiVES: Identify control actions for Voter and SiVES-C

Follow security and privacy TSE guidelines; Authenticate; Accept the privacy agreement; and Vote

Controller Element	Control Action	CA Nr
Voter	- Follow security and privacy guidelines (repeated) - Provide biometric data - Accept the privacy agreement - Vote - Receive voting confirmation - Finalize session	08 13 14 15 16 17

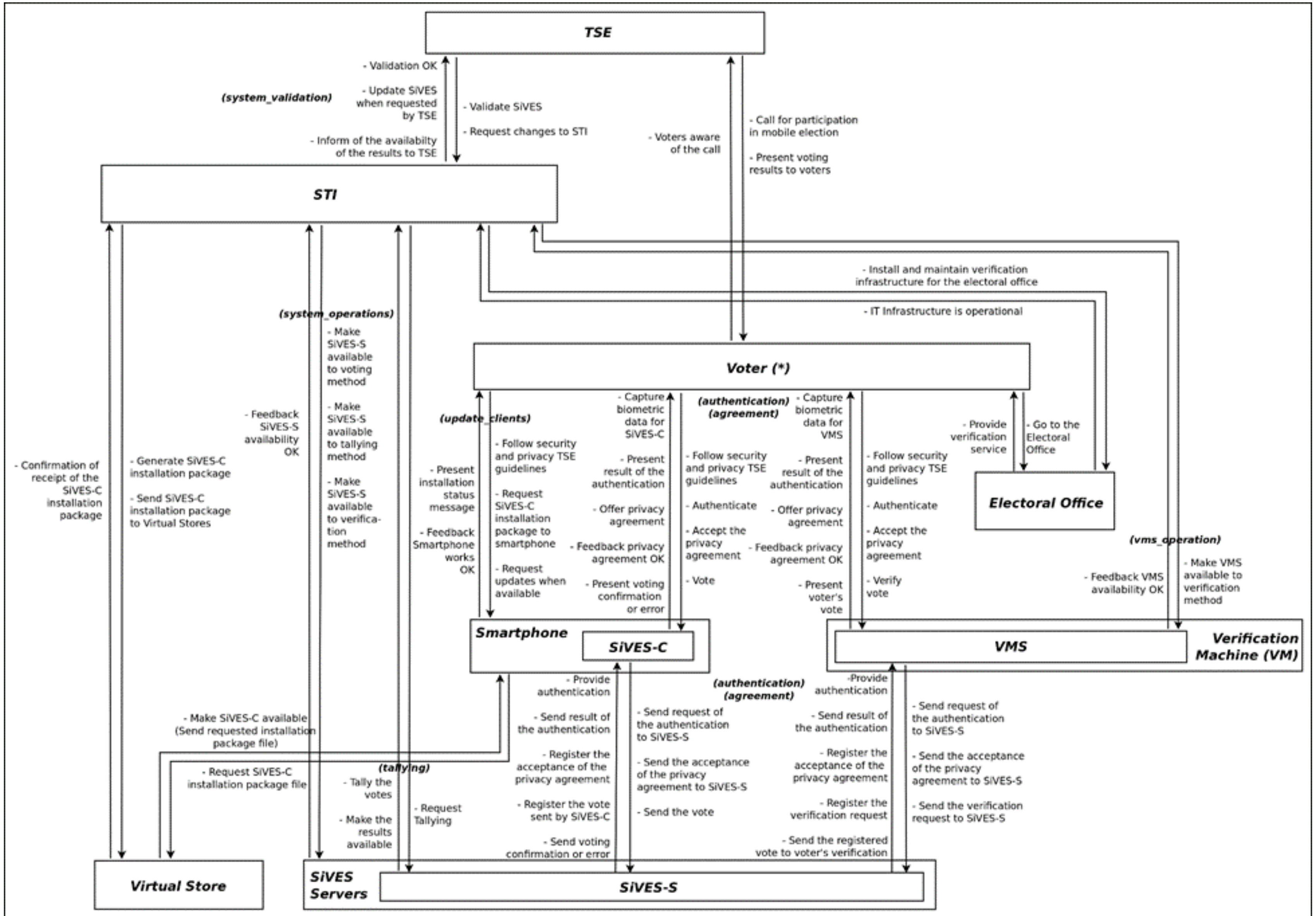
Capture biometric data for SiVES-C; Send request of authentication to SiVES-S; Present result of the authentication; Offer privacy agreement; Send the acceptance of the privacy agreement to SiVES-S; Send the vote; and Present voting confirmation or error

Controller Element	Control Action	CA Nr
SiVES-C	- Capture biometric data for authentication - Send the user's biometric data to SiVES-S - Display the SiVES-S response about user authentication - Offer the privacy agreement to the voter - Send the required acceptance of the privacy agreement to SiVES-S - Send the voter's vote to SiVES-S - Display and store voting confirmation or display error status	18 19 20 21 22 23 24

SiVES: Develop description of the process model

Model Element	CA Nr	Process Model Variable	Values	Sensor or Controlled Process	Hazards
STI	6	sti_validation_status_ok	Yes / No	system_validation	H1, H3, H4
SiVES-S	15, 19, 23	sives_s_available_status_ok	Yes / No	system_operations	H1 to H4
	15, 23, 27, 29	sives_s_authenticated_user	Yes / No	Authentication	H1 to H4
SiVES-C	15, 18	sives_c_updated_in_virtual_stores	Yes / No	update_clients	H3.1, H3.2, H4.1
	18, 25	sives_c_is_installed_and_updated	Yes / No	update_clients	H1, H3, H4
VMS	38	vms_available_status_ok	Yes / No	vms_operation	H2
Voter	29	voter_accepted_privacy_agreement	Yes / No	Agreement	H1.1, H2 to H4

Functional Control Structure


TSE
- Validation OK
(system_validation)
- Update SiVES when requested by TSE
- Inform of the availabilty of the results to TSE
- Validate SiVES
- Request changes to STI
- Voters aware of the call
- Call for participation in mobile election
- Present voting results to voters
STI
- Install and maintain verification infrastructure for the electoral office
- IT Infrastructure is operational
(system_operations)
- Make SiVES-S available to voting method
- Make SiVES-S available to tallying method
- Make SiVES-S available to verifica-tion method
- Feedback SiVES-S availability OK
Voter (*)
- Confirmation of receipt of the SiVES-C installation package
- Generate SiVES-C installation package
- Send SiVES-C installation package to Virtual Stores
(update_clients)
- Present installation status message
- Feedback Smartphone works OK
- Follow security and privacy TSE guidelines
- Request SiVES-C installation package to smartphone
- Request updates when available
- Capture biometric data for SiVES-C
- Present result of the authentication
- Offer privacy agreement
- Feedback privacy agreement OK
- Present voting confirmation or error
(authentication)
(agreement)
- Follow security and privacy TSE guidelines
- Authenticate
- Accept the privacy agreement
- Vote
- Capture biometric data for VMS
- Present result of the authentication
- Offer privacy agreement
- Feedback privacy agreement OK
- Present voter's vote
- Follow security and privacy TSE guidelines
- Authenticate
- Accept the privacy agreement
- Verify vote
- Provide verification service
- Go to the Electoral Office
Electoral Office
(vms_operation)
- Feedback VMS availability OK
- Make VMS available to verification method
Smartphone
SiVES-C
VMS
Verification Machine (VM)
- Make SiVES-C available (Send requested installation package file)
- Request SiVES-C installation package file
(tallying)
- Tally the votes
- Make the results available
- Request Tallying
- Provide authentication
- Send result of the authentication
- Register the acceptance of the privacy agreement
- Register the vote sent by SiVES-C
- Send voting confirmation or error
(authentication)
(agreement)
- Send request of the authentication to SiVES-S
- Send the acceptance of the privacy agreement to SiVES-S
- Send the vote
-Provide authentication
- Send result of the authentication
- Register the acceptance of the privacy agreement
- Register the verification request
- Send the registered vote to voter's verification
- Send request of the authentication to SiVES-S
- Send the acceptance of the privacy agreement to SiVES-S
- Send the verification request to SiVES-S
Virtual Store
SiVES Servers
SiVES-S

(*) Although there are user and voter terms in this presentation and they distinguish the role of user before authenticated (user) and user already authenticated in SiVES (voter), they must be understood like voter in all analysis.

Evaluation of the approach

- The evaluation of the approach consisted of performing the Step 1 and analyzing the results.
- Step 1
  - For each controller, we analyze each control action to find when it is hazardous. To help the discovery of the cases, we use Context Tables.
  - A context table is defined as the combination of all process model variables and values, with issuance of control action.

SiVES: Context table for the control action SiVES-C sends the vote to SiVES-S

CA Nr 23: SiVES-C sends the voter's vote to SiVES-S			
Variables		Control Action provided	Control Action not provided
sives_s_authenticated_user	sives_s_available_status_ok		
Yes	Yes		H1.1
Yes	No	H1.1	
No	Yes	H1.1, H3.1, H4.2	
No	No	H1.1, H3.1, H4.2	

SiVES: Excerpt of context table for the control action “Voter votes”: 4 first entries

CA Nr 15: Voter votes					
Variables					
sives_s_authenticated _user	sives_s_available _status_ok	sives_c_is_installed_and updated	voter_accepted privacy_agreement	Control Action provided	Control Action not provided
Yes	Yes	Yes	Yes		H3.1, H4.2
Yes	Yes	Yes	No	H3.2, H3.3, H4	
Yes	Yes	No	Yes	H3.2, H3.3, H4	
Yes	Yes	No	No	H3.2, H3.3, H4	

CA	Hazardous Control Action (CA with a context: variables with value)	Associated Constraint	Hazards
06	STI provided send SiVES-C installation package file to Virtual Stores when sti_validation_status_ok is no (provided)	STI must not send installation package to virtual stores when the app is not validated by TSE.	H1, H3, H4
15	Voter provided vote when sives_s_available_status_ok is no or sives_s_authenticated_user is no or sives_c_is_installed_and_updated is no or voter_accepted_privacy_agreement is no (provided)	Voter must not be allowed to vote if the server is not available or the voter is not authenticated or the updated app is not installed or the voter has not accepted the privacy agreement.	H3.2, H3.3, H4
18	SiVES-C provided capture biometric data for authentication when sives_c_updated_in_virtual_stores is yes and sives_c_is_installed_and_updated is no (provided)	App must not capture biometric data for authentication if the app is updated in virtual store, but the updated app is not installed.	H3.1, H3.2, H4.1
19	SiVES-C provided send the user's biometric data to SiVES-S when sives_s_available_status_ok is no (provided)	App must not send biometric data to server if server is not available to receive.	H1
23	SiVES-C provided send the voter's vote to SiVES-S when sives_s_authenticated_user is no (provided)	App must not send vote to server if the user is not authenticated.	H1.1, H3.1, H4.2
25	SiVES-S provided receive biometric user data when sives_c_is_installed_and_updated is no (provided)	Server must not receive biometric user data if the app is not updated.	H1
27	SiVES-S provided response, informing whether the user is authenticated as a voter, when sives_s_authenticated_user is no (provided)	SiVES-S must not provide response, informing whether the user is authenticated as a voter, when sives_s_authenticated_user is no .	H1
29	SiVES-S provided receive and store the vote from SiVES-C when sives_s_authenticated_user is no voter_accepted_privacy_agreement is yes (provided)	Server must not receive and store the vote from app if the user is not authenticated, even if the user accepted the privacy agreement.	H3.1, H3.3
38	Electoral Office provided provide verification service when vms_available_status_ok is no (provided)	Electoral Office must not provide verification service if the verification machine server is not available.	H2
39	Voter provided verify the vote when sives_s_available_status_ok is no or sives_s_authenticated_user is no or voter_accepted_privacy_agreement is no (provided)	Voter must not be allowed to verify the vote if the server is not available or the voter is not authenticated or the voter has not accepted the privacy agreement.	H2, H3.1, H4

Results

INFORMATION	QUANTITY
Unacceptable Losses	5
Hazards	13
Constraints	11
Control Actions	41
Hazardous Control Actions	81

Hazardous Control Action due to	Quantity
H1 (Reli, **Avail**, Mission)	**17**
H2	7
H3 (Security)	1
H4 (Privacy)	2
H1 and H2	4
H1 and H3	2
H1 and H4	2
H2 and H3	0
H2 and H4	1
H3 and H4	**29**
H1, H2 and H3	1
H1, H2 and H4	0
H1, H3 and H4	**6**
H2, H3 and H4	**7**
Total	81

Analysis

- Control actions that are hazardous due to H3 (security hazards) account for 46 and 42 of them are also hazardous due to H4 (data privacy hazards).
  - There are 4 HCAs due to H3 that are not due to H4.
  - This result shows that when a control action is hazardous to security, it is generally hazardous to privacy.
- The result also shows that these 4 HCAs require specific focus on security issues.

Analysis

- For instance, the hazardous control action **SiVES-S does not overwrite previous vote in case of "revoting"** may lead to the state that allows for undue alteration of the voter's vote (H3.3) if the new vote is different from the previous vote.

CA	Hazardous Control Action due to privacy violation and not security violation	Hazards due to
04	TSE does request changes of SiVES to STI	H1, H2, H3.2
27	SiVES-S does not respond, informing if the user is authenticated as a voter when sives_s_authenticated_user is yes	H1.1, H3.1, H3.2
29	SiVES receives and stores the vote from SiVES-C when sives_s_authenticated_user is No and voter_accepted_privacy_agreement is Yes	H3.1, H3.3
30	**SiVES-S does not overwrite previous vote in case of "revoting"**	H1.1, H3.3

Most of HCAs due to Privacy but not Security are related to the correct processing of data privacy agreement.

CA	Hazardous Control Action due to privacy violation and not security violation	Hazards due to
14	Voter does not accept the **privacy agreement**	H4
19	SiVES-C (or VMS) does not send the user's biometric data to SiVES-S when sives_s_available_status_ok is Yes	H1.1, H4.1
22	SiVES-C (or VMS) does not send the required **acceptance of the privacy agreement** to SiVES-S	H4
28	SiVES-S does not register the acceptance of **the privacy agreement**	H2, H4
29	SiVES receives and stores the vote from SiVES-C when sives_s_authenticated_user is Yes and **voter_accepted_privacy_agreement** is No	H1.1, H4.2

Concluding Remarks

- The proposed STAMP-based approach, with STPA-Sec Step 1, allows identifying safety, security and privacy hazardous control actions and associated constraints.
- We observed that in general control actions that are hazardous due to security issues are also hazardous due to privacy issues and vice-versa.
- We did not identify security and privacy requirements yet. We are emplying STRIDE and LINDDUN for this. We have some preliminary results.

Preliminary results using STPA Scenarios, Information Life Cycle, and STRIDE

Result	**Quantity**
Unacceptable Losses	5
Hazards	13
Constraints	11
Control Actions	41
Hazardous Control Actions	82
Scenarios + STRIDE	26 **+ 16 (61,5%)**
Associated Security Constraints	82
Requirements + STRIDE	26 **+ 23 (88,5%)**

2019 STAMP Workshop
March, 25-28, 2019, MIT, Cambridge

http://sunnyday.mit.edu/

USING STAMP FOR ANALYSIS OF SECURITY AND DATA PRIVACY

Nívio P. Souza, ITA

Cecília A. C. Cesar, ITA

Juliana M. Bezerra, ITA

Celso Massaki **Hirata**, ITA- **hirata@ita.br**