Security and Safety Engineering Qualitative Assessment Report by Dimitar Bachvarov

EXECUTIVE SUMMARY

I have decided for the report to focus on the new software and the information that is inside each vote as they are the key to a successful election. From there 4 different primary assets and another 4 supporting assets were created and I ultimately aim to find a way to protect them.

After the Impact and Likelihood evaluation few key problems were identified and were put against a Risk table and the overall risk evaluation. From there I recommended the five most important threats that we need to focus on as they present the highest risk out of them all.

Having the above mentioned threats in mind some controls need to be put in place to prevent security attacks on our election. From all the solutions some stood out as more effective or easier to implement as such I have recommended them as a starting point.

Work submitted in partial fulfilment for the course of Security and Safety Engineering – Vrije Universiteit Amsterdam - a.a. 2022/2023

This work is original work, has been done by the undersigned student and has not been copied or otherwise derived from the work of others not explicitly cited and quoted. The undersigned student is aware that plagiarism is an offence which may lead to failure of the course and more severe sanctions.

NAME, SURNAME Dimitar Bachvarov

Risk Assessment Report
On
The Votes Counting Software Case Study

1. TARGET OF EVALUATION

We are presented with the case regarding the election and more specifically the new counting aspect of the new software soon to be implemented with a centralised network system. As we review this paper our main points of protection must be the new software and the information that is inside each vote as they are the key to a successful election. So having said that, for the assignment I consider as the target of evaluation the ability to correctly gather and count the votes of the people.

2. SUMMARY OF FINDINGS

I have identified as a key asset the service provided by the software as the consequences after a thread are the most severe. The second key asset should be the data in the votes and their integrity as this is what the public is the most interested about while it being the most sensitive for the presented case.

For every PA there should be a tangible secondary asset(SA). In this report I have discovered 4 main SAs which are as follows:

1. Central hub servers
2. Staff
3. Electronics
4. Software

After that I have established an impact score on the triad(C,I,A). With some of the assets scoring high scores on the matter. Then a wide range of threats were chosen to “test” and re-review all the information gathered before to establish a new more finely graded impact score. Likelihood is an important part of any report as it puts all the threats against how likely something is to occur. Some highly likely examples are: Fire, Unauthorised Access to IT systems, Lack of resources, Manipulation of Hardware or Software and Software Vulnerabilities or Errors which had high likelihood scores. Final risk score is computed by combining all the information from the previous findings. For that reason a special Risk table was created by using the quantitative method as it provides fine grading. In the end after the risk evaluation the “High” risk threats are: Unauthorised Access to IT Systems, Lack of Resources, Malfunction of Devices or Systems and Manipulation of Hardware or Software which I recommended for immediate correction.

For the threat controls I have established some solutions for the known threats. I would recommend implementing first the said pre-controls:

- Information stored in multiple different locations
- Two-factor authentication process
- Good resource management
- Maintenance / repair on regular basis
- Implementation of security functions

And post-controls:

- Data recovery procedures
- Protocol for immediate password termination
- Procedure of redirection of the public
- Procedure for replacement of the malfunctioning equipment
- Disabling and containing the infiltrated part of the software

As they bring the highest results while solving the highest risk threats.

3. RISK ANALYSIS

3.1. Impact Assessment

Table 1.1: Primary Asset (PA) Identification

1.1 Primary Asset (PA) Identification			
Primary Asset ID	**Primary Asset Description**	**Type (information or service)**	**Justification**
Voting	The voting service provided by the new system and equipment	Service	This is the core feature regarding voting related softwares and it is one of the most looked after by the public.
Votes	The votes that are chosen by the public	Information	The votes are the most important thing that we need to protect as they contain sensitive information about the future of a nation.
Personal data	The information of every person who votes	Information	In the profiles there is personal information of million of people that is connected with their votes as they are justifying them
The counting process	The counting service provided by the new software.	Service	It is crucial to protect the integrity of the software to ensure fair and efficient counting.

I assume that all the voters and the staff surrounding the case would do their work optimally and with no mistakes which otherwise would increase the impact score for the performance and capacity in some of the cases.

3.2. Supporting Asset Identification & Valuation

In this step we are finding out which of the triad (C,I,A) is responsible for the biggest impact on our primary assets. To calculate this we ran it through multiple categories such as Personnel or Branding while finally selecting the biggest overall score to be its representative.

Table 1.2: Impact Assessment on Primary Assets

Key observations are the serious branding hits that would occur if any problems occur during the whole process as the whole nation's eyes are placed upon this event.

1.2 Impact Assessment on Primary Assets										
Primary Asset ID	**Potential Compromise of C, I or A**	**Impact (see Table in Methodology)**								
		Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulatory**	**Environment**	**Overall impact**	**Justification**
Voting	C	1	1	1	1	1	1	1	1	There would not be a problem if it is disclosed the way the public is voting. Matter of fact is that it is as openly as possible.
	I	3	1	2	4	5	2	1	5	In case of tampering with the voting system the public will lose fate in it causing riots (which could cause casualties) damaging the name of the country and its economy in the process.
	A	3	2	5	3	4	1	1	5	If not available, the voting would be rescheduled with backlash from the public which could lead to serious branding damage and protest (which could cause casualties) as people will lose trust in the government.
Votes	C	1	1	1	3	4	4	2	4	If it becomes known who are you going to vote for it would be a breach of trust for some members of the public. This most certainly will infringe on the regulatory practices while even slightly damaging the environment as they will scrap all the votes to start anew.
	I	3	1	1	4	5	5	2	5	If the integrity of the votes is illegally damaged there would be catastrophic backlash from the public filled with protests (which could cause casualties) demolishing the name of the country while forcing a costly redo of the election.
	A	1	2	4	4	3	2	2	4	If the results were upheld from the public for more than the agreeable time this could be as a result of a performance issue or manipulative actions which would cost huge resources (mainly needing to redo the entire expensive election) and substantially damage the branding of the country in the process as the media would .
Personal data	C	4	1	1	1	4	3	1	4	If personal information is leaked then this will be extremely damaging for the country's brand while potentially damaging a lot of the voters. Not only that but protests around the country will occur in response to the breach of security (which could cause casualties).
	I	3	1	3	1	3	3	1	3	Substantial problems in performance will occur as the authentication of those data would lead to a lot of errors which will void votes while creating branding and regulatory problems in the process. Not only that but protests around the country will occur in response to the breach of security (which could cause casualties).
	A	3	1	4	3	4	1	1	4	The personal data could not be hidden from the voters but this would slow down the process of counting / verifying the votes which could be damaging for the branding of the country as it could lead to costly delays Not only that but protests around the country will occur in response to the breach of security (which could cause casualties).
The counting process	C	1	2	2	3	3	1	1	3	As the source code is presented to the public there would be little to no problems disclosing information about the software.
	I	1	4	5	3	5	1	1	5	One of the most damaging things is for the integrity of the counting software to fail resulting in massive capacity and performance problems when switching to manual while damaging the trust and the brand of the country.

	A	1	4	4	3	4	1	1	4	To withhold the service that this asset provides is more or less the same as damaging its integrity with slight decreases in sensitivity as it could not lead to redoing the whole process or creating huge waves of mistrust from the public

Table 2.1: Linkage of Support Assets with Primary Assets

Finding out key supporting assets that correspond to the primary assets is crucial for this task as this is the only way to know how to protect those intangible services or data. There are different varieties of supporting assets that could lead to damages of the primary ones with the staff being one of the most prominent ones as it directly connects with almost every primary asset.

Linkage with Primary Assets						
Supporting Assets		**Primary Assets**				**Justification**
ID	**Description**	Voting	Votes	Profiles	The counting process	
Central hub servers	The central server room where all the information is stored	indirect	direct	direct	indirect	If the place where all the information is damaged the whole system will be crippled. As it contains the profiles and the votes it has direct connection with them.
Staff	The on field workers	direct	direct	direct	indirect	The workers have the most important part of the operation as they control the flow of information regarding everything except the quality of the software provided.
Electronics	The electronics in every municipalities	direct	direct	indirect	indirect	If the technology is not in optimal conditions this will affect the voting process and the new data flow while the profiles could be collected from other documents.
Software	The new counting software that is present in the system.	indirect	direct	indirect	direct	If there is a problem (caused by the software) with the main counting program the result would be invalid.

3.3 Threat Evaluation

For this step I will take all the information that I have discovered from the previous tables to find the good amount of logical threats that can interact directly with the supporting assets, damaging them in the process in one way or another.

I have covered a wide range of threats from natural disasters (Fire) to malware attacks (Manipulation of Hardware or Software).

Some notable examples could be:

- Manipulation of Information
- Sabotage
- Unauthorised Access to IT Systems
- Malfunction of Devices or Systems
- Lack of Resources
- Manipulation of Hardware or Software

As they still end up holding a high impact score even after a more detailed review. The reason for that could be because of the lack of prevention / controls put in place or the ones that are implemented are not as effective as they must be to prevent or at least patch such a vulnerability. Later down in the document more perspectives will be put in place and as a result, some of the threats that are mentioned above might be overthrown by others.

Table 3.1: Threat Impact

We can observe that a good amount of threads after the review have less of an impact as I first thought. The reason for this is the already established protections that cover a lot of the basic cases.

Impact of Vulnerabilities & Threat Scenarios Evaluation																	
Supporting Asset	**Threat**	**Vulnerability**	***Primary Assets***												**Inherited Impact**	**Reviewed Impact**	**Justification for attenuating circumstances**
			Voting			**Votes**			**Profiles**			**The counting process**					
			C	I	A	C	I	A	C	I	A	C	I	A	MAX	<=	
		Impact ⇨	**1**	**5**	**5**	**4**	**5**	**4**	**4**	**3**	**4**	**3**	**5**	**4**			
Central hub servers	Fire	Incorrect wiring/overheating/humans fault						X			X				4	1	Every modern central hub is equipped with anti-fire systems(Inert Gas Fire Suppression) preventing the problem
	Manipulation of Information	Unauthorised access or malware changing the stored information					X			X					5	4	Variety of measures (authentication cards / malware protections) are in place for such scenarios, reducing the risk.
	Data Loss	Poor backup or recovery system					X	X		X	X				5	3	Copies of the data are usually stored in another place to prevent such actions but there is still a risk if multiple data locations are hit at once.
Staff	Absence of Personnel	Staff being absent unexpectedly due to illness or accident	X		X			X							5	1	Recruiting another staff member would not be difficult to achieve as the entry level of this job is easy to achieve
	Sabotage	A staff intentionally breaking or opposing the rules for benefit		X	X	X	X		X	X					5	4	There is a vetting process for the staff member but it is more simple to bypass it in a small town especially in combination with the previous thread
	Unauthorised Access to IT Systems	Unprotected password/leaked security code	X	X		X	X								5	5	
Electronics	Failure or Disruption of	Power supply failure cutting the			X			X			X				5	3	With enough battery power the technology could withstand the average down

	the Power Supply	amount of electricity needed															time but not if there is a massive problem
	Malfunction of Devices or Systems	Malfunction of the voting equipment			X			X			X				5	5	
	Lack of Resources	Not enough equipment in a municipality			X										5	5	
Software	Manipulation of Hardware or Software	Malware/attack send to the system				X			X			X	X		5	5	
	Software Vulnerabilities or Errors	Undiscovered errors in the software which can crash the system				X						X	X	X	5	2	The software is usually precisely checked and optimised with enough edge cases to prevent such thing from happening although it is not impossible
	Bad Planning or Lack of Adaptation	Overwhelming amount of votes that are beyond the counting capacity of the software						X					X	X	5	1	The system should be adapted for the worst case scenario which is the total population in the country which can prevent that from happening

Table 3.2: Threat likelihood

I observed that the opportunity in every cell is the same as the election takes place rarely and finishes within a few days making the class "opportunity" fall in the seldom category! Not only that, but as some of the threads were not led by a human, some of the criterias were considered as non applicable (skills/means for example) and given automatic 5 as in no limitation.

Likelihood Assessment on Supporting Assets											
Supporting Asset	**Threat**	**Vulnerability**	**Likelihood Areas (see Table in the Methodology)**								
			Skills	**Means**	**Opportunity**	**Profit**	**Attention**	**Impunity**	**Detection**	**Overall**	**Justification**
Central hub servers	Fire	Fire caused by incorrect wiring/overheating/humans fault	5	5	2	1	4	5	5	5	As the fire (caused by accident) is not a life actor criterias such as skills/means and profit are without limitations and without profit. But if the threat happens we can expect a huge amount of publicity with no chance of predicting the event and with no one to prosecute for the event.
	Manipulation of Information	Unauthorised access or malware changing the stored information	2	3	2	5	1	1	2	2	A malicious actor would need very good skills, hard to obtain stuff (ID card / powerful and hardly trackable tech), while having a small window of opportunity (only 2 days till election). On the other hand, there is huge profit but to the cost of certainty of punishment if caught by all the protection systems.
	Data Loss	Data accidentally or purposefully deleted or overwritten.	3	3	2	1	5	1	3	3	The skills needed to delete something are less than the ones needed to modify the information while the means and opportunity stays the same. Differently from before the profit would not exist as you do not get anything of it if we exclude massive media attention which is the attacker's goal (the news around the world will cover this as it does not happen often). Punishment if caught is certain but the detection is lower as the attacker would leave less of a cyberprint behind him.
Staff	Absence of Personnel	Staff being absent unexpectedly due to illness or accident	5	5	2	1	2	5	5	3	As this is not a malicious thread but something natural the skills/means/profit would be the same as in the fire thread. The difference would be in the media attention where there would be local media coverage at best and the last 2 categories would not exist as no one is at fault or need to be detected.
	Sabotage	A staff intentionally	5	4	2	1	3	1	2	2	Breaking equipment or requirements requires no certain skills with only need to be part of the staff

		breaking or opposing the rules for benefit									(publicly available) but has no profit, huge risk of detection with certainty to be punished, while only receiving a good amount of local coverage.
	Unauthorised Access to IT Systems	Unprotected password	5	3	2	5	1	2	3	4	There are no specific skills needed to steal a password from somebody higher in the ladder. It is just difficult to find the correct target. But if you find one, the profit is extremely high as you can decide the fate of the election while having no media attention on you. But this comes as a risk of high chance of detection with almost certainty to be prosecuted.
Electronics	Failure or Disruption of the Power Supply	Power supply failure cutting the amount of electricity needed	5	5	2	1	4	5	5	1	Just like with fire, it will be impossible to predict and prosecute, while there is no profit/means/skills in play. The publicity could be throughout the whole country as a result of it being a big event on the election days.
	Malfunction of Devices or Systems	Malfunction of the voting equipment	5	5	2	2	4	5	5	3	It is similar to the previous point. The only difference is the fact that this could lead to the purchase of new equipment which could be considered as a small profit.
	Lack of Resources	Not enough equipment in a municipality	5	5	2	2	3	5	5	4	Similarly in this thread we can see a small amount of profit being made on the back of potential new equipment with less media attention than the power supply thread.
Software	Manipulation of Hardware or Software	Malware/attack send to the system	2	4	2	5	1	5	3	4	Here one would need expert knowledge to attack the system with a fair chance of being caught and 100% chance of being prosecuted for that. On the other hand, there is a big profit with low media attention while it all can be done behind a laptop.
	Software Vulnerabilities or Errors	Undiscovered errors in the software which can crash the system	5	5	2	1	4	3	4	4	One can detect such problems only by chance while this thread brings a lot of attention and no profit as it is not intended. Another thing to be mentioned is once again as the thread is not driven by a life actor the means and skills are limitless but with a chance of prosecuting the firm responsible for the oversight / lack of enough testing,
	Bad Planning or Lack of Adaptation	Overwhelming amount of votes that are beyond the counting capacity of the software	5	5	2	1	4	3	4	2	Finally, here the media attention is once again extremely high with a chance of prosecution against the firm responsible. This thread could be detected only by chance as most of the plans are considered perfected before the impact.

3.4 Risk Evaluation

In this section we will place a multiplication score of all the threats over a risk table to find the final risk level. After that a recommendation of the priority threats will be presented.

Low Risk: A low risk is a security threat that has a low probability of occurring or would have minimal impact on the assets if it occurs.

Medium Risk: A medium risk is a security threat that has a moderate probability of occurring or would have a more substantial impact on the assets if it did occur.

High Risk: A high risk is a security threat that has a high probability of occurring or would have a catastrophic impact on the assets if it did occur.

Table 4.1: Risk table.

To calculate my table, I decided to use the quantitative method/multiplication path (multiplying the values to get the final result in a box). From there, I decided that everything below 8(not included) would be in a low priority, from 8 to 13 (not included) would be medium and everything above that would be critical. Some key things about it are the fact that if something is very unlikely to happen it does not matter how catastrophic it is, as ultimately there should not be a lot of effort put into something with a low probability rate.

Colour code:

Green = Low risk (No priority, could be ignored if there is no resources)

Orange = Medium risk (Weak priority, could be fixed in the closer future but it must not be ignored)

Red = High risk (High priority, should be fixed immediately)

Risk table with Reviewed Impact					
Likelihood	**1. No impact, NA**	**2. Minor**	**3. Severe**	**4. Critical**	**5. Catastrophic**
5. Certain	Low (5)	Medium (10)	High (15)	High (20)	High (25)
4. Very likely	Low (4)	Medium (8)	Medium (12)	High (16)	High (20)
3. Likely	Low (3)	Low (6)	Medium (9)	Medium (12)	High (15)
2. Unlikely	Low (2)	Low (4)	Low (6)	Medium (8)	Medium (10)
1. Very Unlikely	Low (1)	Low (2)	Low (3)	Low (4)	Low (5)

Table 4.2: Risk evaluation

One can observe that both categories must be in the critical range to be considered high risk level as if that is not the case the overall result is quite substantially reduced (as the logic dictates).

Risk evaluation					
	Threats (T 3.1)	**Vulnerability (T3.1)**	**Reviewed Impact (T3.1)**	**Likelihood (T3.2)**	**Risk Level (T4.1)**
Central hub servers	Fire	Fire caused by incorrect wiring/overheating/humans fault	1	5	Low (5)
	Manipulation of Information	Unauthorised access or malware changing the stored information	4	2	Medium (8)
	Data Loss	Poor backup or recovery system	3	3	Medium (9)
Staff	Absence of Personnel	Staff being absent unexpectedly due to illness or accident	1	3	Low (3)
	Sabotage	A staff intentionally breaking or opposing the rules for benefit	4	2	Medium (8)
	Unauthorised Access to IT Systems	Unprotected password	5	4	High (20)

Electronics	Failure or Disruption of the Power Supply	Power supply failure cutting the amount of electricity needed	3	1	Low (3)
	Malfunction of Devices or Systems	Malfunction of the voting equipment	5	3	High (15)
	Lack of Resources	Not enough equipment in a municipality	5	4	High (20)
Software	Manipulation of Hardware or Software	Malware/attack send to the system	5	4	High (20)
	Software Vulnerabilities or Errors	Undiscovered errors in the software which can crash the system	2	4	Medium (8)
	Bad Planning or Lack of Adaptation	Overwhelming amount of votes that are beyond the counting capacity of the software	1	2	Low (2)

Recommendations:

From the table above our priority should be to tackle problems that have "High" risk levels. In my case those are:

- ★ Staff:
  - Unauthorised Access to IT Systems
- ★ Electronics:
  - Lack of Resources
  - Malfunction of Devices or Systems
- ★ Software:
  - Manipulation of Hardware or Software

As they are either very likely or with a chance to cause serious impact this is a great starting point for us to go over all the vulnerabilities if time and resources allow. Later down the road "Medium" risk level should be next in line as they are less time sensitive.
One "Medium" risk example that should be taken first into consideration (as it has a score of 9 which is the highest of them) is:

- ★ Central Hub Servers
  - Data Loss

3.5. Risk Treatment

In this part of the document, I will present some controls that, if implemented, are going to prevent some vulnerability from manifesting or in the worst case it will reduce the likelihood and or the impact that said threats creates.

Some notable mentions are:

Pre-controls:

- Information stored in multiple different locations
- Two-factor authentication process
- Good resource management
- Maintenance / repair on regular basis
- Implementation of security functions

And post-controls:

- Data recovery procedures
- Protocol for immediate password termination
- Procedure of redirection of the public
- Procedure for replacement of the malfunctioning equipment
- Disabling and containing the infiltrated part of the software

Those once achieved the most optimal results and should be considered first for implementation, especially if the budget is not big enough to cover all the expenses.

The one who is going to be responsible for managing and paying for the systems is going to be mentioned after the control itself but they are ultimately going into one of two categories:

- ☑ Done by Kiesraad
- ☑ Done by Municipalities

Table 5.1: Risk Treatment and Calculation of Residual Risk for Supporting Assets

For this step I now take the recommended threats in the previous step and establish some controls to prevent/recover as much as possible. This table could also serve as a visual summary as all the columns are filled with information from throughout the report.

Risk Treatment and Calculation of Residual Risk for Supporting Assets										
Supporting Assets (T2.1)	**Threats (T4.1)**	**Vulnerability (T4.1)**	**Pre-Controls**	**Post-Controls**	**Reviewed Impact (T4.1)**	**Likelihood (T4.2)**	**Residual Impact**	**Residual Likelihood**	**Residual Risk (T4.1)**	**Justification**
Central hub servers	Data Loss	Poor backup or recovery system	Information stored in multiple different locations. (Done by Kiersraad)	Implement data recovery procedures to restore lost data from backups or other sources. (Done by Kiersraad)	3	3	1	1	Low(1)	After storing the data in multiple differently located servers the chance of them all failing is slim to none, while having a backup makes the impact not significant enough to cause a problem which overall makes the threat none critical.
			Training personnel on data loss prevention. (Done by Kiersraad)	Updating the servers to be more robust to mistakes in the future. (Done by Kiersraad)	3	3	2	2	Low(4)	Although a create alternative (demotes the risk level again to Low) this is not as effective as the previous, because a trained person could still make a mistake while updating the system might not always cover all the errors. Ultimately both factors are slightly tuned down for those reasons.
Staff	Unauthorised Access to IT Systems	Unprotected password	Physical protection system, such as life guards and CCTV around restricted areas. (Done by Municipalities)	Logging system that records activities. (Done by Kiersraad)	5	4	4	3	Medium(12)	This combination of controls would make the threat less risky but still not good enough as although the chance of stealing/overhearing the password is lower ultimately it is not nearly as impossible while the logging system would be only able to present which

										password was stolen and when it was used.
			Two-factor authentication process to access the system. (Done by Kiersraad)	Protocol for immediate password termination. (Done by Kierstraat)	5	4	2	1	Low(2)	If both controls were to be implemented the probability of this threat occuring shrinks to almost none which makes both the likelihood and the impact go down
Electronics	Lack of Resources	Not enough equipment in a municipality	Good resource management before the election. (Done by Municipalities)	Procedure of redirection of the public to the nearest best location. (Done by Municipalities)	5	4	2	1	Low(2)	If both controls are implemented the municipalities are to be covered almost entirely by this threat, because with good planning resources can be reallocated for new equipment while in the worst case scenario part of the public can be allocated to the nearest best option reducing the impact and the likelihood alike.
	Malfunction of devices or systems	Malfunction of the voting equipment	Maintenance / repair on a regular basis on existing technology. (Done by Municipalities)	Procedure for replacement of the malfunctioning equipment. (Done by Municipalities)	5	3	1	1	Low(1)	Regular maintenance could prevent malfunctions of most system and devices which decreases the probability of this threat of happening while in the cases that it does occur immediate replacement would prevent a lot of future problems
Software	Manipulation of Hardware or Software	Malware/attack send to the system	Implementation of security functions in the IT application. (Done by Kiersraad)	Disabling and containing the infiltrated part of the software. (Done by Kiersraad)	5	4	2	2	Low(4)	Implementation of security functions that are preventing malware to infect the system is going to decrease the likelihood of this happening. Not only that, but having emergency containment protocol in place would be beneficial if something

										passes through the defences which is still a possibility as everything that is made by a human can be broken by a human.
			Exhausting testing against most commonly known malwares /attacks. (Done by Kiesraad)	Constant monitoring of the system for out of normal behaviour. (Done by Kiesraad)	5	4	4	2	Medium(8)	Exhausting tasting is always useful especially in the early stages of development. Unfortunately, they are usually not enough to prevent exploitation of an undiscovered vulnerability or error. On the other hand, the implementation of the second control is cheap and effective as one can scan for out of normal computational power being used which often leads to illegal activity (this drags the likelihood score down as the chance of detection skyrockets).

Recommendation on how should be proceeded from here, I have given in the summary of findings.

4. ACKNOWLEDGMENTS

Everything on this report is created only by me. Apart from some useful information provided by the peer reviews and with the help of the BSI Threat Catalogue (From where I found the needed information for part of the report) this document is mine to the latter.

REFERENCES (EXAMPLES)

[1] Fröhlich, B. and Plate, J. 2000. The cubic mouse: a new device for three-dimensional input. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (The Hague, The Netherlands, April 01 - 06, 2000). CHI '00. ACM, New York, NY, 526-531. DOI= http://doi.acm.org/10.1145/332040.332491.

[2] Tavel, P. 2007. *Modelling and Simulation Design*. AK Peters Ltd., Natick, MA.

[3] Sannella, M. J. 1994. *Constraint Satisfaction and Debugging for Interactive User Interfaces*. Doctoral Thesis. UMI Order Number: UMI Order No. GAX95-09398., University of Washington.

[4] Forman, G. 2003. An extensive empirical study of feature selection metrics for text classification. *J. Mach. Learn. Res*. 3 (Mar. 2003), 1289-1305.

[5] Brown, L. D., Hua, H., and Gao, C. 2003. A widget framework for augmented interaction in SCAPE. In P*roceedings of the 16th Annual ACM Symposium on User Interface Software and Technology* (Vancouver, Canada, November 02 - 05, 2003). UIST '03. ACM, New York, NY, 1-10. DOI= http://doi.acm.org/10.1145/964696.964697.