



Zero effort security for the home PC users?

By Terje Risa



Outline

- Introduction
- Project description
- Choice of method
- Experimental work
- Preliminary analysis
- Conclusion



Introduction

- Most users are not willing to invest much effort in securing their home PC.
- Increasing use of Internet, to access sensitive information, online banking etc.
- Internet related crime is growing.



Introduction

- Home PC users needs usable and practically secure solutions.
- Service providers might help home users protecting their computers with user-friendly security software.
- The usability of the products are important in order for them to be used.



Introduction

“Systems must be not only secure, but useably and practically secure.”

-Dourish et. al. [1]



Introduction

- What is usability?
 - Jakob Nielsen describes it as:
 - Easy to learn
 - Efficient to use
 - Easy to remember
 - Few errors
 - Subjectively pleasing



Project description

- Evaluating the usability and security to some selected security products.
- Investigate if the notion of zero effort security for home PC users is possible.



Project description

- These products must address the Norwegian home PC user population.
 - Internet Security Suites available in Norwegian were therefore chosen.
 - These security suites provided a all-in-one solution.



Choice of method

- Usability evaluation method
 - Needed a resource economical method:
 - Heuristic evaluation.
 - Cognitive walkthrough
- Heuristic evaluation were chosen.



Choice of method

- Security testing
 - Testing anti-malware solutions.
 - Gathering data from independent security evaluations.
 - Security certificates achieved.



Experimental work

- The usability experiment:
 - 11 participants performing a heuristic evaluation on each of the four products.
 - The participants scored Nielsen's heuristics (usability principles) on a scale from 1-5.
 - After each product were evaluated, did they answer a System Usability Scale.



Experimental work

- Nielsen's heuristics included in the experiment:
 - Visibility of system status
 - Match between system and real world
 - User control and freedom
 - Consistency and standards
 - Recognition rather than recall memory
 - Flexibility and efficiency of use
 - Aesthetic and minimalist design



Experimental work

- Security testing
 - A small sample of malware were collected and tested against the products.
 - Firewall leak testing



Preliminary Analysis

	Heuristic evaluation checklist									
Product	1.1	1.2	2	3.1	3.2	4	5	6	7	Total Σ
1	3.81	3.72	3.27	3.54	3.63	3.72	3.72	3.54	3.72	3.63
2	3.54	3.09	4.09	3.63	2.90	3.63	3.45	3.45	3.63	3.49
3	2.63	2.45	3.45	3.27	3.09	2.81	2.36	2.72	2.81	2.84
4	4.27	4	4.27	3.36	3.45	4.27	3.81	4	3.63	3.89

Table 5: Overall evaluation score for the products.



Preliminary Analysis

- System Usability Scale, a 'quick and dirty' usability scale from 0-100:
 - Product 1 – Average score of 63.4
 - Product 2 – Average score of 63.4
 - Product 3 – Average score of 38.2
 - Product 4 – Average score of 72.7



Preliminary Analysis

- Security testing:
 - Small malware sample:
 - Product 1 – Detected 184/184
 - Product 2 – Detected 24/184
 - Product 3 – Detected 24/184
 - Product 4 – Detected 84/184
 - Note: Product 2 and 3 couldn't scan the "large" file containing virus. This file should maybe not be included, since product 4 also had some troubles with it.



Preliminary Analysis

- Firewall Leak test:
 - Substitution: Product 2 passed, the rest failed.
 - Launcher: All product failed.
 - DLL injection: Product 1 and 4 passed, 2 and 3 failed.
 - Process injection: All product failed.
 - Registry injection: All product failed.
 - Windows messaging: All product failed.
 - Note: All the products were installed with default settings.



Preliminary Analysis

- Independent anti-malware testing:
 - From AV-comparatives.org:

Malware categories	Products		
	F-Secure Anti-Virus 8.0	Norman Security Suite 7.0	Norton Anti-Virus 15.0
Windows viruses	99,7%	94.4%	~100%
Macro viruses	~100%	99.8%	100%
Script viruses	98.7%	75.3%	98.4%
Worms	99.2%	97.1%	99.8%
Backdoors/Bots	97.3%	94.8%	96.0%
Trojan	96.5%	93.2%	97.3%
Other malware	96.9%	77.5%	97.6%
Total	97.5%	94.2%	97.7%

Table 10: AV-comparatives on-demand test from February 2008.



Conclusion

Definition, from Whitten and Tygar[2]:

Security software is usable if the people who are expected to use it:

- 1. are reliably made aware of the security tasks they need to perform;
- 2. are able to figure out how to successfully perform those tasks;
- 3. don't make dangerous errors; and
- 4. are sufficiently comfortable with the interface to continue using it.



Conclusion

- There appears to be some differences between the products usability.
- There appears to be some differences between the products security.
- Some of the product are made to minimize the user-intervention as much as possible, which might explain the bad results in the firewall leak tests.



Conclusion

- Zero effort security for home PC users?
 - Security suites can possibly move towards this notion; especially together with up-to-date programs and educating the users to act careful.



Thank you for your attention!

- Questions?



Bibliography

- [1] Dourish, P., Grinter, E., de la Flor, J. D., & Joseph, M. 2004. *Security in the wild: user strategies for managing security as an everyday, practical problem*. Personal Ubiquitous Comput., 8(6), 391–401.
- [2] Whitten, A. & Tygar, J. D. 1999. *Why johnny can't encrypt: a usability evaluation of pgp 5.0*. In SSYM'99: Proceedings of the 8th conference on USENIX Security Symposium, 14–14, Berkeley, CA, USA. USENIX Association.