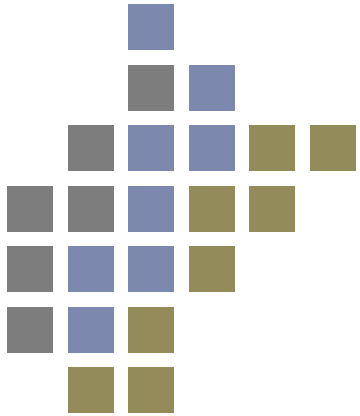
Countermeasures against Malicious Software

Martin Boldt

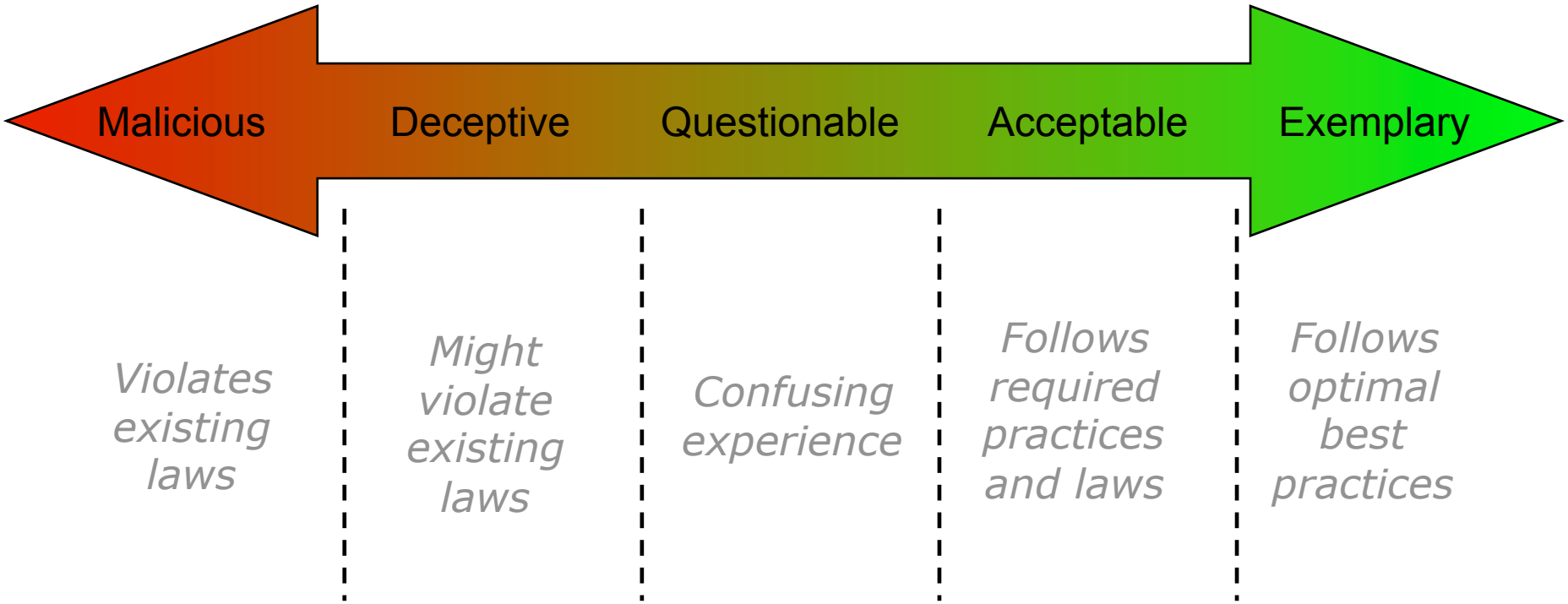
School of Engineering

Blekinge Institute of Technology

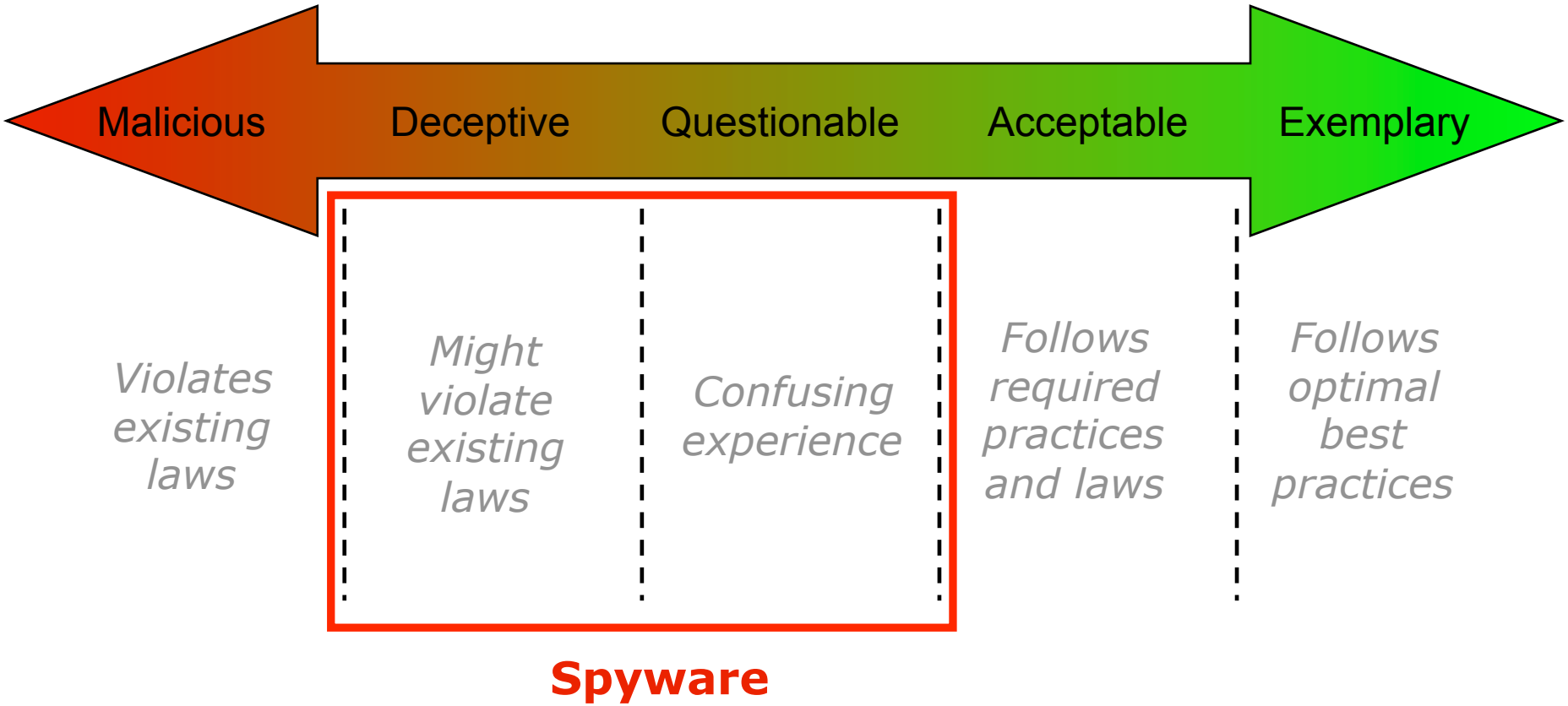
martin.boldt@bth.se



Software Behaviour

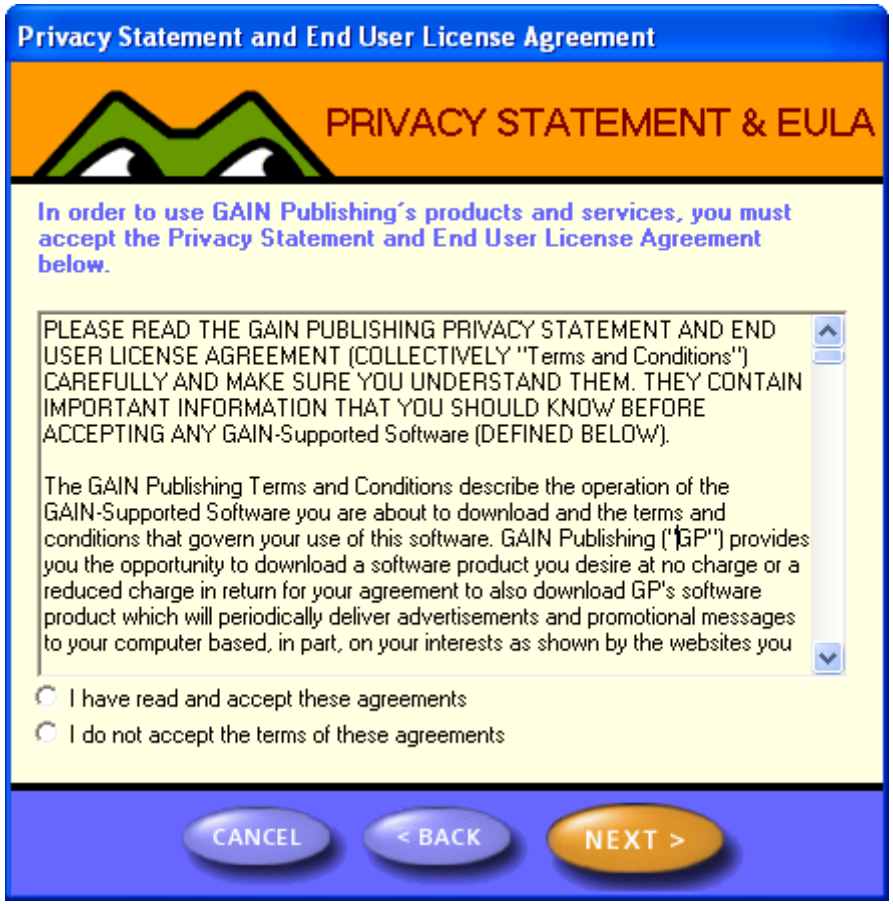


Software Behaviour

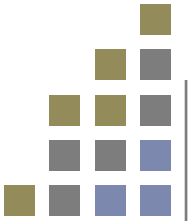


The Spyware Problem (i)

- We use the Gator software as an example of what users face on the Internet
- During the installation users face an End User License Agreement (EULA)
- It contains 6,645 words and is presented in a small window
- Would you read it?



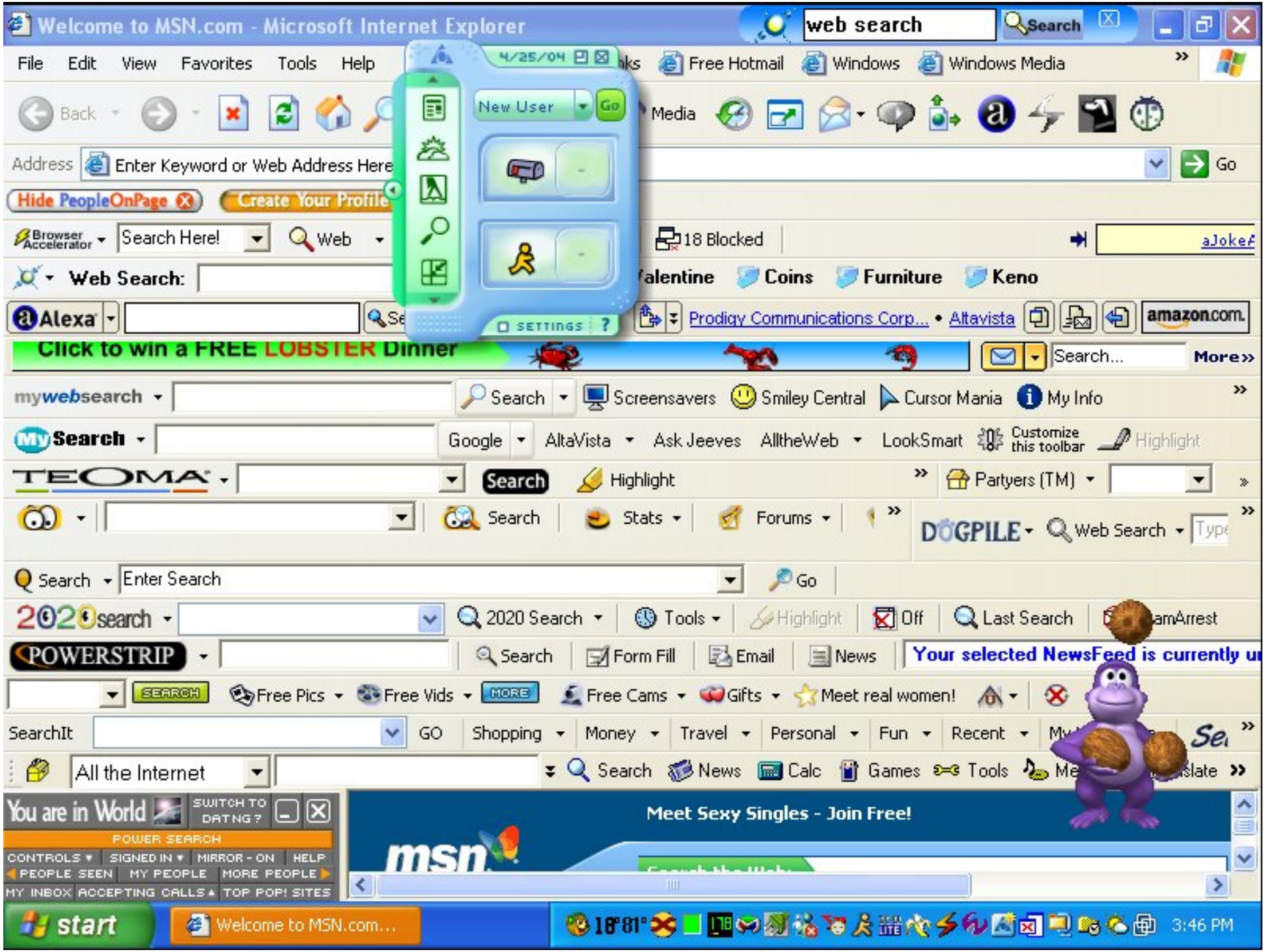
Blekinge Institute of Technology
SE-372 25 Ronneby
+46 455 38 50 00
www.bth.se/eng

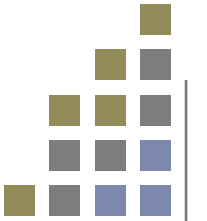


The Spyware Problem (ii)

- The EULA reveals that the following programs are installed:
  - eWallet
  - Precision Time
  - Date Manager
  - Offer Companion
  - Weatherscope
  - SearchScout Toolbar
- Such programs create large revenues for the their developers
- Spyware corporations report annual revenues in excess of $50 Million each

Blekinge Institute of Technology
SE-372 25 Ronneby
+46 455 38 50 00
www.bth.se/eng

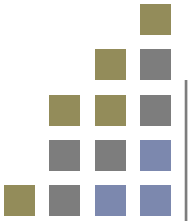

Welcome to MSN.com - Microsoft Internet Explorer
web search
Search
File Edit View Favorites Tools Help
Free Hotmail
Windows
Windows Media
Back
Address
Enter Keyword or Web Address Here
Go
Hide PeopleOnPage
Create Your Profile
Search Here!
Web
18 Blocked
Web Search:
Valentine
Coins
Furniture
Keno
Alexa
Prodigy Communications Corp...
Altavista
amazon.com
Click to win a FREE LOBSTER Dinner
Search...
More»
mywebsearch
Search
Screensavers
Smiley Central
Cursor Mania
My Info
MySearch
Google
AltaVista
Ask Jeeves
AlltheWeb
LookSmart
Customize this toolbar
Highlight
TEOMA
Search
Highlight
Partyers (TM)
Search
Stats
Forums
DOGPILE
Web Search
Search
Enter Search
Go
2020search
2020 Search
Tools
Highlight
Off
Last Search
POWERSTRIP
Search
Form Fill
Email
News
Your selected NewsFeed is currently u
SEARCH
Free Pics
Free Vids
MORE
Free Cams
Gifts
Meet real women!
SearchIt
GO
Shopping
Money
Travel
Personal
Fun
Recent
All the Internet
Search
News
Calc
Games
Tools
You are in World
SWITCH TO DATING?
POWER SEARCH
CONTROLS
SIGNED IN
MIRROR - ON
HELP
PEOPLE SEEN
MY PEOPLE
MORE PEOPLE
MY INBOX
ACCEPTING CALLS
TOP POP! SITES
Meet Sexy Singles - Join Free!
msn
start
Welcome to MSN.com...
3:46 PM



Software Reputation System (i)

- Similar reputation systems are being successfully used by for instance Amazon.com and IMDb.com
- We put forward the idea of using *collaborative reputation systems* to help inform users about the effects of software
- Gather previous users' knowledge about software and present it to the new user
- Users provide ratings and comments for the software they use most frequently
- This information is sent to a central repository where it is transformed into *software reputations*

Blekinge Institute of Technology
SE-372 25 Ronneby
+46 455 38 50 00
www.bth.se/eng



Software Reputation System (ii)

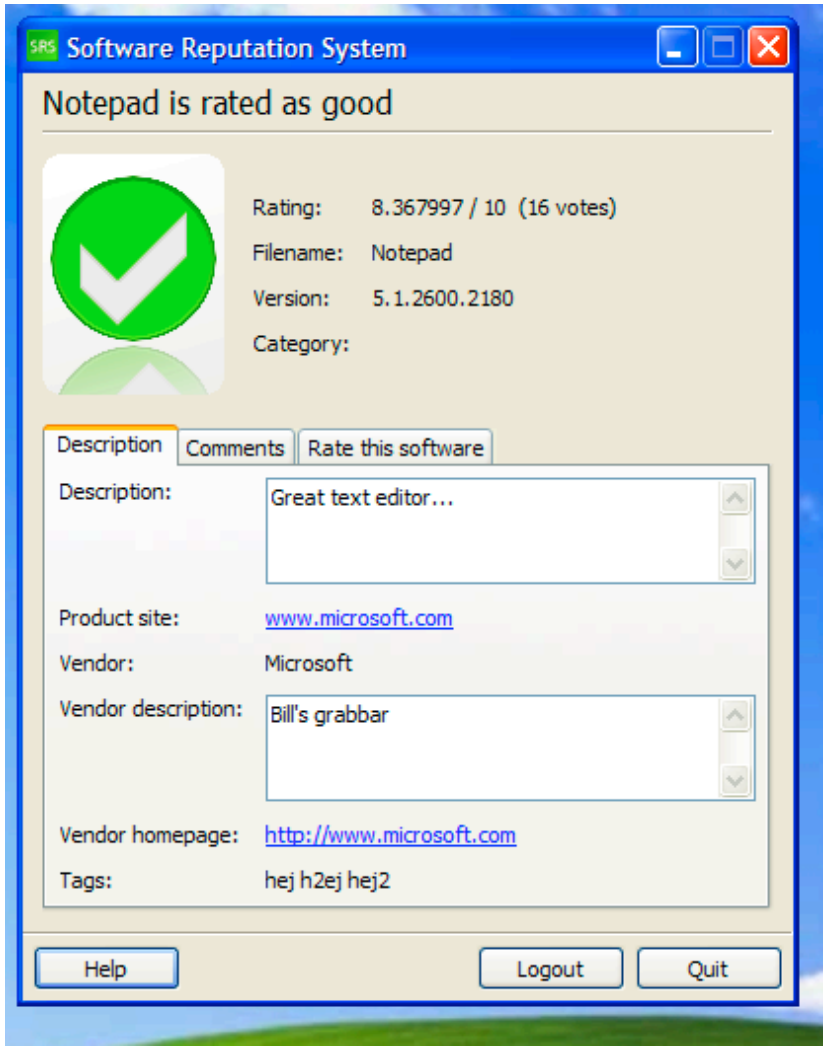
- When a new user is about to install a software he/she is presented with the software reputation
- The software reputation allows the user to make a more informed decision regarding the software installation
- This protection is *preventive* since the user make this decision before the software is allowed to execute
- To mitigate antagonistic intentions from users we make use of *trust factors* and *meta ratings*

Blekinge Institute of Technology
SE-372 25 Ronneby
+46 455 38 50 00
www.bth.se/eng

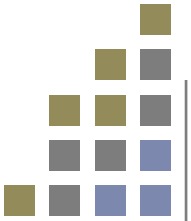
Software Reputation System (iii)

- We are developing a proof-of-concept tool which is integrated into Microsoft Explorer software
- A beta version will be available in late November

www.softwareputation.com



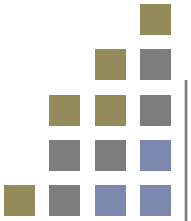
Blekinge Institute of Technology
SE-372 25 Ronneby
+46 455 38 50 00
www.bth.se/eng



EULA analysis (i)

- Spyware distributors typically mention in the End User License Agreement (EULA) if their application hosts spyware
  - The main reason seems to be to avoid legal repercussions
  - The EULA act as a last escape route in court
- EULAs are notoriously difficult for normal computer users to understand
- However, we believe it is possible for computers to exploit the fact that spyware hosting is mentioned in in the EULA

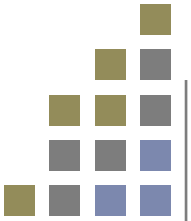
Blekinge Institute of Technology
SE-372 25 Ronneby
+46 455 38 50 00
www.bth.se/eng



EULA analysis (ii)

- Inspired by spam filtering services we apply data miners (classification algorithms) to classify EULAs as good or bad
- Data miners generalize from training examples of EULAs with known classification
- We generated a data set by collecting 1000 programs with EULAs and classifying each EULA as either good or bad
  - 900 good and 100 bad programs and EULA
- Then we evaluated 15 popular classification algorithms using this data set

Blekinge Institute of Technology
SE-372 25 Ronneby
+46 455 38 50 00
www.bth.se/eng



State-of-the-art tools

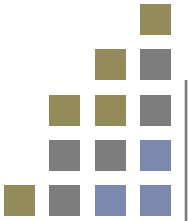
- There exist one web based EULA analyzing services that rely on “simple” keyword matching
- The tools assign a score related to the number of found spyware keywords
- The actual classification of software as either spyware or legitimate is very much up to the user

Blekinge Institute of Technology
SE-372 25 Ronneby
+46 455 38 50 00
www.bth.se/eng

Results

Algorithm	Accuracy % correct	AUC	Training Time seconds	Testing Time seconds
AdaBoostM1	73.82(5.79) ●	0.78(0.04) ●	3.55(0.28)	0.00(0.01)
DecisionStump	68.82(11.11)	0.69(0.11)	0.33(0.08)	0.00(0.00)
HyperPipes	76.47(7.59) ●	0.90(0.07) ●	0.04(0.01)	0.07(0.09)
IBk	77.94(5.59) ●	0.78(0.06) ●	0.04(0.01)	0.13(0.02)
J48	73.24(10.23) ●	0.73(0.10) ●	1.29(0.23)	0.00(0.01)
JRip	71.18(5.33) ●	0.72(0.07) ●	2.02(0.23)	0.00(0.00)
KStar	59.71(4.17) ●○	0.68(0.07) ●	0.00(0.00)	9.20(0.42)
NaiveBayes	79.41(9.80) ●	0.80(0.10) ●	0.31(0.02)	0.11(0.05)
NaiveBayesNominal	**93.94(6.42) ●+**	**0.92(0.06) ●**	**0.03(0.01)**	**0.00(0.01)**
PART	72.65(10.74) ●	0.72(0.11) ●	2.41(2.15)	0.00(0.01)
RandomForest	75.29(7.10) ●	0.83(0.08) ●	3.64(0.20)	0.00(0.00)
RBFNetwork	77.35(7.73) ●	0.78(0.09) ●	1.46(0.19)	0.17(0.02)
Ridor	67.65(11.35)	0.68(0.11)	0.87(0.11)	0.00(0.01)
SMO	**95.53(1.97) ●+**	**0.82(0.08) ●**	**0.25(0.08)**	**0.00(0.00)**
VotedPerceptron	81.47(6.66) ●	0.87(0.07) ●	0.04(0.01)	0.02(0.01)
ZeroR (baseline)	50.00(0.00)	0.50(0.00)	0.00(0.01)	0.00(0.00)
EULA analyzer	72.7 (3.86)	N/A	N/A	N/A

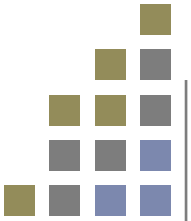
Blekinge Institute of Technology
SE-372 25 Ronneby
+46 455 38 50 00
www.bth.se/eng



Evaluating the technique

- Using data miners to distinguish between legitimate software and spyware is absolutely possible
  - 2 miners perform significantly better than the state-of-the-art web service
- Accuracy could be even further increased by tweaking the classifier algorithms to the problem at hand
  - In our experiments all algorithms executed with the default settings
- This technique could be implemented in a tool that automatically detects and analyze EULAs and present the result to the user

Blekinge Institute of Technology
SE-372 25 Ronneby
+46 455 38 50 00
www.bth.se/eng

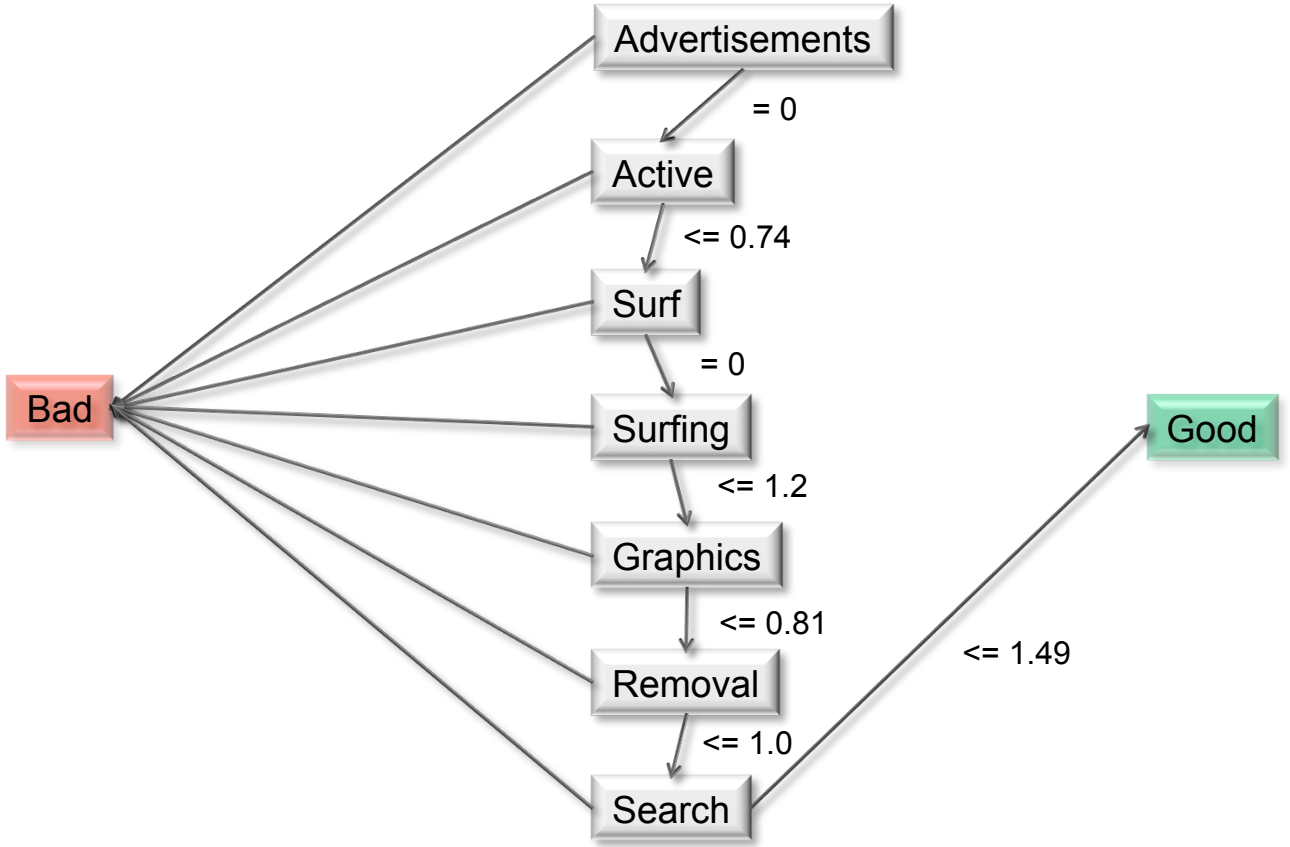


Conclusion

- We believe that EULA analyzer tools and a software reputation system can greatly help users handle malicious software
- Further research is required when it comes to mitigating antagonistic intentions among “bad users”
- A new PhD student financed by .SE will focus on this in beginning of 2009

Blekinge Institute of Technology
SE-372 25 Ronneby
+46 455 38 50 00
www.bth.se/eng

Example of the J4.8 algorithm



Blekinge Institute of Technology
SE-372 25 Ronneby
+46 455 38 50 00
www.bth.se/eng