The effect of competition intensity on software security

An empirical analysis of security patch release on the web browser market

Arrah-Marie Jo

Telecom Paristech

WEIS 2017

Main question

- The larger the market share of a software, the greater the probability for a security failure to be exploited.
- A more concentrated market → more security risks? (The danger of monoculture e.g. Stamp 2004; Böhme 2005; Schneier 2010)
- But how about software vendors security investment behavior?
- To answer to this question, we study the relationship between **competition intensity** and software vendors' **responsiveness in releasing security patches**.

Main question

- The larger the market share of a software, the greater the probability for a security failure to be exploited.
- A more concentrated market → more security risks? (The danger of monoculture e.g. Stamp 2004; Böhme 2005; Schneier 2010)
- But how about software vendors security investment behavior?
- To answer to this question, we study the relationship between **competition intensity** and software vendors' **responsiveness in releasing security patches**.

Main question

- The larger the market share of a software, the greater the probability for a security failure to be exploited.
- A more concentrated market → more security risks? (The danger of mono-culture e.g. Stamp 2004; Böhme 2005; Schneier 2010)
- But how about software vendors security investment behavior?
- To answer to this question, we study the relationship between **competition intensity** and software vendors' **responsiveness in releasing security patches**.

Empirical strategy

- We study the case of the **web browser market**:
  - A market at the heart of web security issues
  - A software provided free of charge to users, a major element of today digital market strategies (Monopolkommission, 2015)
- We use two aspects that reflects the competition intensity in the market:
  - Market concentration
  - Dominance of a firm

Empirical strategy

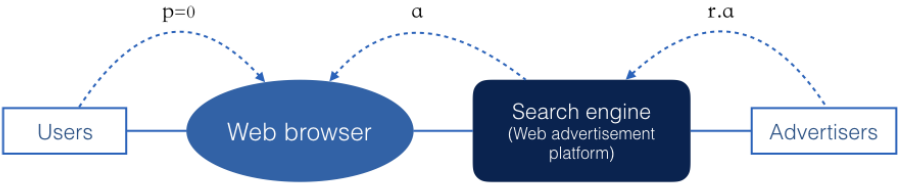
- We study the case of the **web browser market**:
  - A market at the heart of web security issues
  - A software provided free of charge to users, a major element of today digital market strategies (Monopolkommission, 2015)
- We use two aspects that reflects the competition intensity in the market:
  - Market concentration
  - Dominance of a firm

Web browser publishers derive their revenue from search engines

Browser	Publisher	Rendering engine	License	Revenue model
Chrome	Google	Blink (fork of Webkit)	Proprietary software with open source rendering engine (GNU LPGL). An open source version of the browser is available (Chromium)	90% of ABC's revenues come from search related ad.
Firefox	Mozilla	Gecko	Open source (MPL)	Built-in search engine royalties ($>$ 90% of whole revenues, $\simeq$100M$) and donations
Internet Explorer	Microsoft	Trident and EdgeHTML since 2015	Proprietary	Revenues from other activities
Safari	Apple	Webkit	Proprietary software with open source rendering engine (GNU LPGL)	1B$ of built-in search engine royalties from Google (in 2014)

Sources: Wikipedia, Bloomberg.com for Apple, official annual financial statement reports for Mozilla and Google

A model (1/4)



What is the security quality that a firm choose to provide, considering:

1. The number of firms competing in the market
2. Firms' installed base of loyal consumers

A model (2/4)

Assumptions:

- Symmetric firms except for the size of their installed base of loyal consumers
- Consumer's utility depends only on security quality
- the per-capita revenue is exogenous
- Marginal cost is equal to zero
- Cost function for security investments is increasing and convex in security quality

A model (3/4)

There are n firms. Firm i chooses its security quality s_i and has a share of loyal consumers $b_i \in [0,1]$. We note $\sum_{i=1}^{n} b_i = B$ $(B \leqslant 1)$.

Firm i's profit is:

$$\pi_i = a\left[b_i + (1-B)\frac{s_i}{\sum_{j=1}^{n} s_j}\right] - \frac{\phi s_i^2}{2}$$

The security quality in equilibrium is:

$$s_i^* = \sqrt{(1-B)\cdot\frac{n-1}{n^2}\cdot\frac{a}{\phi}}$$

A model (4/4)

If we assume that only firm k has an installed base, $B = b_k = \alpha_k m_k$, where $m_k \in (0,1]$ firm k's market share and $\alpha_k \in (0,1]$ the share of loyal consumers among its consumer, then:

$$s_k^* = \sqrt{(1 - \alpha_k m_k)\frac{n-1}{n^2} \cdot \frac{a}{\phi}}$$

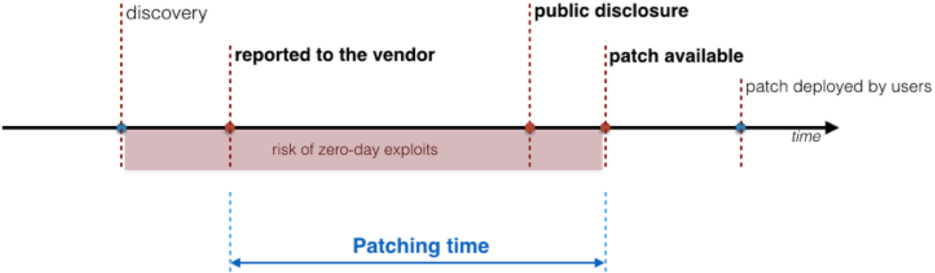
Conclusion from the model

From the model, we propose that:

- In a market where firms compete in security quality, market concentration has a positive effect on the security level provided by a firm ($\frac{\partial s_i}{\partial n} < 0$).
- The security quality chosen by a highly dominant firm i decreases with respect to its market share ($\frac{\partial s_i}{\partial m_i} < 0$).
- When a firm highly dominates the market then the positive effect of market concentration on the security level it provides is reduced ($\frac{\partial s_i}{\partial m_i \partial n} < 0$).

Patching time as a proxy of the security quality

Figure: *Security vulnerability life cycle*

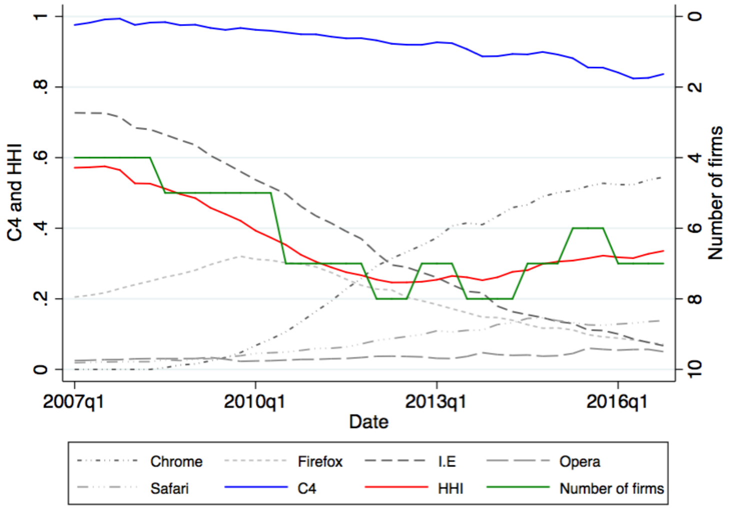


The econometric model

$$\begin{aligned} patching\_time = {} & \beta_0 + \beta_1 concentration \\ & + \beta_2 X_{Vuln} + \beta_3 X_{Vend\&Soft} + \beta_4 disclosure + \beta_5 time\_trend + \epsilon \end{aligned} \tag{1}$$

$$\begin{aligned} patching\_time = {} & \beta_0 + \beta_{1a} concentration \\ & + \beta_{1b} big\_mshare + \beta_{1c} concentration \cdot big\_mshare \\ & + \beta_2 X_{Vuln} + \beta_3 X_{Vend\&Soft} + \beta_4 disclosure + \beta_5 time\_trend + \epsilon \end{aligned} \tag{2}$$

Main explanatory variables (1/2): Market concentration measures

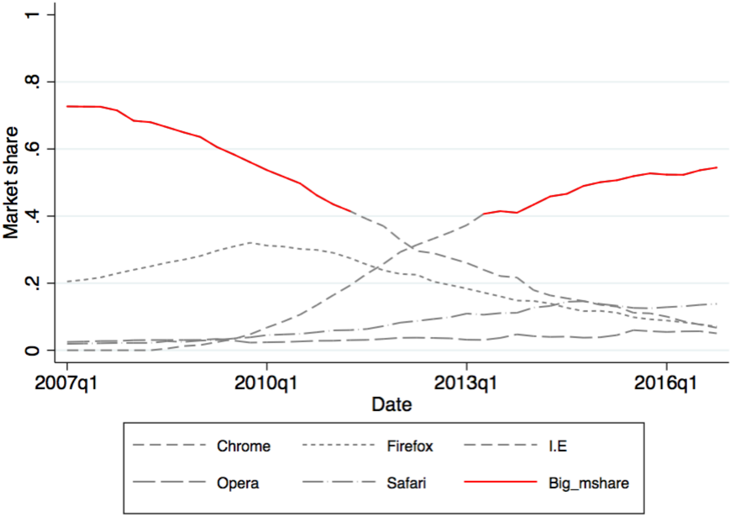


The econometric model

$$
\begin{aligned}
patching\_time = &\beta_0 + \beta_1 concentration \\
&+ \beta_2 X_{Vuln} + \beta_3 X_{Vend\&Soft} + \beta_4 disclosure + \beta_5 time\_trend + \epsilon
\end{aligned} \tag{3}
$$

$$
\begin{aligned}
patching\_time = &\beta_0 + \beta_{1a} concentration \\
&+ \beta_{1b} big\_mshare + \beta_{1c} concentration \cdot big\_mshare \\
&+ \beta_2 X_{Vuln} + \beta_3 X_{Vend\&Soft} + \beta_4 disclosure + \beta_5 time\_trend + \epsilon
\end{aligned} \tag{4}
$$

Main explanatory variables (2/2): *Big_mshare*



The econometric model

$$
\begin{aligned}
patching\_time =& \beta_0 + \beta_1 concentration \\
& + \beta_2 X_{Vuln} + \beta_3 X_{Vend\&Soft} + \beta_4 disclosure + \beta_5 time\_trend + \epsilon
\end{aligned} \tag{5}
$$

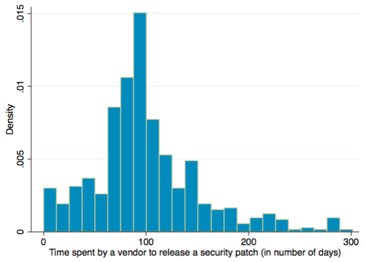
$$
\begin{aligned}
patching\_time =& \beta_0 + \beta_{1a} concentration \\
& + \beta_{1b} big\_mshare + \beta_{1c} concentration \cdot big\_mshare \\
& + \beta_2 X_{Vuln} + \beta_3 X_{Vend\&Soft} + \beta_4 disclosure + \beta_5 time\_trend + \epsilon
\end{aligned} \tag{6}
$$

Data

- 586 vulnerabilities affecting Web browsers, reported from January 2007 to December 2016 from 3 different projects: Google Project Zero, Zero Day Initiative, and iDefense
- We consider the patch release time of the four principal browsers: Internet Explorer, Safari, Firefox, Chrome.
- Only vulnerabilities assigned to web browser publishers
- Enrichment with other databases
  - NVD & MITRE: public disclosure date, severity of the vulnerability, type of vulnerability
  - From each vendor: version release date, vulnerability patching date
  - Statcounter.com: evolution of market share
  - ITU ICT Indicators database : evolution of number of internet users

Regression models

- One observation: a web browser vulnerability assigned to a web browser publisher
- OLS & Negative Binomial model
  - Data fits well with the OLS model assumptions
  - Count model can be used (*Patching_time* is a positive integer), but we have 586 observations and the mean value is relatively distant from 0 (*mean* = 100.2)
    → Results of **Linear** and **Negative Binomial** regressions are compared
  - No additional value with a survival model



Results (1/4)

Using as main expl. variable:	$-n$		HHI	
	OLS (coef.)	NB (AME)	OLS (coef.)	NB (AME)
Concentration	-5.483**	-4.794**	-85.35**	-114.3***
	(2.422)	(2.314)	(42.14)	(42.00)
Vulnerability specific variables (*vulnerability_severity*, vulnerability type dummies)				
Soft. and vendor specific variables (*software_age*, vendor dummies)	All control variables are included			
Disclosure effect variables				
Time effect variables				
Observations	586	586	586	586
R-squared	0.388		0.386	
Wald chi-squared		236.43		239.51

Robust Standard errors
*** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$
For OLS estimation, coefficients are reported. For NB, average marginal effects are reported.

Results (2/4)

Big_mshare = 1 when:	market share ⩾ 0.40		market share ⩾ 0.45		market share ⩾ 0.50	
	OLS (coef.)	NB (IRR)	OLS (coef.)	NB (IRR)	OLS (coef.)	NB (IRR)
Concentration	-5.361**	0.932**	-5.496**	0.924***	-5.850**	0.914***
	(2.552)	(0.0265)	(2.561)	(0.0263)	(2.602)	(0.0260)
Big_mshare	42.45	5.939***	21.33	8.925***	34.01	22.02***
	(34.78)	(2.367)	(42.03)	(4.227)	(51.62)	(12.72)
Big_mshare	8.942	1.298***	4.349	1.435***	6.998	1.738***
#Concentration	(5.447)	(0.0847)	(7.376)	(0.123)	(9.489)	(0.190)
Vulnerability specific						
Soft. and vendor specific						
Disclosure effect	All control variables are included					
Time effect variables						
Observations	586	586	586	586	586	586
R-squared	0.394		0.388		0.389	
Wald chi-squared		241.40		239.96		246.04

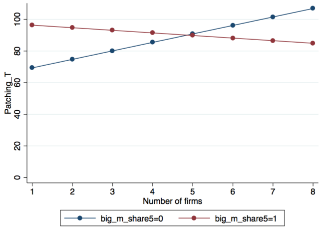
Robust Standard errors

*** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$

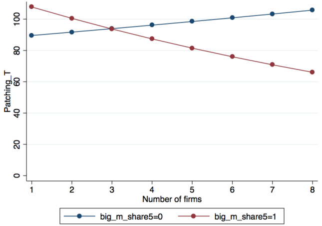
For OLS regressions coefficients are reported. For NB regressions IRR are reported.

Results (3/4): interaction between *concentration* and *Big_mshare*

Big_mshare = 1 when the web browser's market share is greater than 0.50

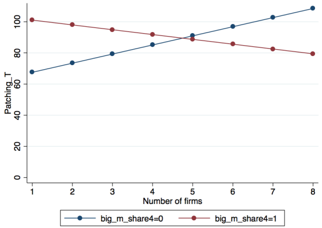


(OLS)

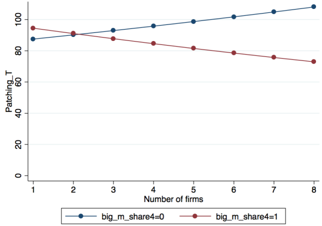


(NB)

Big_mshare = 1 when the market share is greater than 0.40



(OLS)



(NB)

Results (4/4): Impact of public disclosure of vulnerability information & open source component

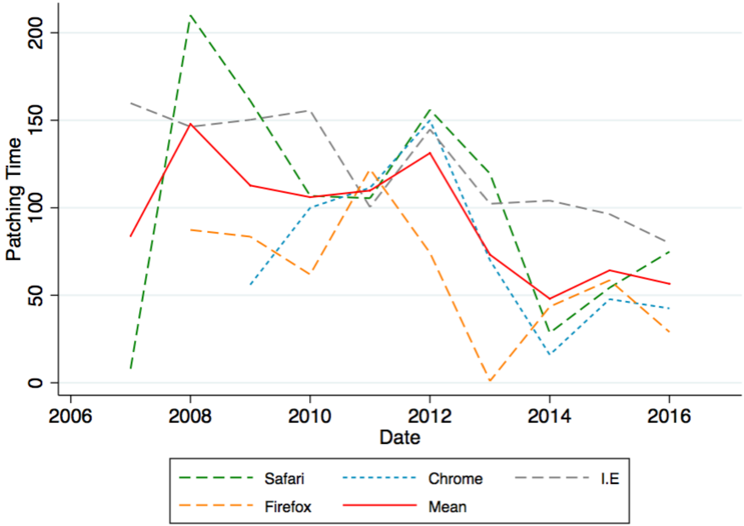
Concentration:	**-*n***		***HHI***		**-*n***	
Big_mshare = 1:					market share $\geqslant 0.50$	
	(OLS)	(NB)	(OLS)	(NB)	(OLS)	(NB)
disclosure	-49.59***	-49.56***	-49.87***	-50.19***	-49.64***	-50.26***
	(3.563)	(4.449)	(3.580)	(4.465)	(3.545)	(4.460)
open_source	-17.53***	-22.46***	-18.40***	-23.64***	-16.10**	-23.75***
	(5.352)	(5.327)	(5.295)	(5.253)	(6.466)	(6.319)
	All other variables are included except for vendor dummies					
Observations	586	586	586	586	586	586
R-squared	0.384		0.383		0.386	
Wald chi-squared		232.37		235.06		239.15

Robust Standard errors
*** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$
For OLS estimation, coefficients are reported. For NB, average marginal effects are reported.

Conclusion

- Main findings:
  - Market concentration is not necessarily harmful to vendors security provision behavior.
  - Explanation: here, firms compete in web browser's (security) quality because revenues come from web browsing traffic
  - However, the positive effect of market concentration is less clear when a firm is highly dominant.
- The closest paper to ours: Arora et al. (2010) Competition and patching of security vulnerabilities: An empirical analysis. *Information Economics and Policy*
- No other theoretical or empirical studies on quality vs. competition of free products/software

Appendix 1


Patching Time
0
50
100
150
200
2006
2008
2010
2012
2014
2016
Date
Safari
Chrome
I.E
Firefox
Mean

using as *Concentration*:	*-n*		*HHI*	
	OLS	NB	OLS	NB
Concentration	-5.483**	-4.794**	-85.35**	-114.3***
	(2.422)	(2.314)	(42.14)	(42.00)
vulnerability_severity	-5.210**	-5.308**	-5.704***	-6.219**
	(2.050)	(2.567)	(2.188)	(2.593)
vulnerability_type dummies				
*cwe*119 (Improper Restriction of Operations [...])	-6.874	-3.904	-7.152	-3.399
	(10.65)	(10.50)	(10.63)	(10.46)
...	...	...	...	...
*cwe*704 (Incorrect type conversion or cast)	-8.606	-8.168	-7.544	-5.299
	(11.15)	(46.92)	(11.13)	(48.28)
software_age	0.755*	0.795	0.789*	0.798
	(0.438)	(0.530)	(0.442)	(0.527)
apple	-10.11	-13.92**	-11.54*	-14.95**
	(6.888)	(6.838)	(6.884)	(6.696)
google	-23.21*	-31.13***	-23.46*	-32.61***
	(12.16)	(7.648)	(12.01)	(7.526)
mozilla	-23.98***	-26.37***	-24.65***	-27.78***
	(8.303)	(6.776)	(8.172)	(6.645)
disclosure	-48.64***	-48.37***	-48.99***	-49.04***
	(3.611)	(4.462)	(3.631)	(4.474)
qyear	-1.513***	-1.513***	-1.605***	-2.276***
	(0.293)	(0.293)	(0.316)	(0.659)
Constant	458.7***		549.1***	
	(71.85)		(90.34)	
Observations	586	586	586	586
R-squared	0.388		0.386	
Wald chi-squared		236.43		239.51
VIF for *Concentration*	1.40		1.68	

Robust standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1