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 $\rightarrow$ 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.
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

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

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 $\sum_{i=1}^{n} b_i = B$ ($B \leq 1$).

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:

$$
s_i^* = \sqrt{(1 - B) \cdot \frac{n - 1}{n^2} \cdot \frac{a}{\phi}}
$$
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 \( \frac{\partial s_i}{\partial m_i, \partial n} < 0 \).
The effect of competition intensity on software security

Introduction

A model

Empirical strategy

Data

Results

Conclusion
Patching time as a proxy of the security quality

Figure: *Security vulnerability life cycle*
The econometric model

\[ \text{patching\_time} = \beta_0 + \beta_1 \cdot \text{concentration} \]
\[ \quad + \beta_2 X_{\text{Vuln}} + \beta_3 X_{\text{Vend\&Soft}} + \beta_4 \text{disclosure} + \beta_5 \text{time\_trend} + \epsilon \]  (1)

\[ \text{patching\_time} = \beta_0 + \beta_{1a} \cdot \text{concentration} \]
\[ \quad + \beta_{1b} \text{big\_mshare} + \beta_{1c} \text{concentration} \cdot \text{big\_mshare} \]
\[ \quad + \beta_2 X_{\text{Vuln}} + \beta_3 X_{\text{Vend\&Soft}} + \beta_4 \text{disclosure} + \beta_5 \text{time\_trend} + \epsilon \]  (2)
Main explanatory variables (1/2): Market concentration measures
The econometric model

\[ patching\_time = \beta_0 + \beta_1 concentration \]
\[ + \beta_2 X_{Vuln} + \beta_3 X_{Vend\&Soft} + \beta_4 disclosure + \beta_5 time\_trend + \epsilon \] (3)

\[ patching\_time = \beta_0 + \beta_{1a} concentration \]
\[ + \beta_{1b} big\_mshare + \beta_{1c} concentration \cdot big\_mshare \]
\[ + \beta_2 X_{Vuln} + \beta_3 X_{Vend\&Soft} + \beta_4 disclosure + \beta_5 time\_trend + \epsilon \] (4)
Main explanatory variables (2/2): *Big_mshare*
The econometric model

\[ \text{patching} \cdot \text{time} = \beta_0 + \beta_1 \text{concentration} \]
\[ + \beta_2 X_{\text{Vuln}} + \beta_3 X_{\text{Vend\&Soft}} + \beta_4 \text{disclosure} + \beta_5 \text{time\_trend} + \epsilon \]  

(5)

\[ \text{patching} \cdot \text{time} = \beta_0 + \beta_{1a} \text{concentration} \]
\[ + \beta_{1b} \text{big\_mshare} + \beta_{1c} \text{concentration} \cdot \text{big\_mshare} \]
\[ + \beta_2 X_{\text{Vuln}} + \beta_3 X_{\text{Vend\&Soft}} + \beta_4 \text{disclosure} + \beta_5 \text{time\_trend} + \epsilon \]  

(6)
1 Introduction

2 A model

3 Empirical strategy

4 Data

5 Results

6 Conclusion
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
1 Introduction

2 A model

3 Empirical strategy

4 Data

5 Results

6 Conclusion
## Results (1/4)

Using as main expl. variable:

<table>
<thead>
<tr>
<th></th>
<th>OLS (coef.)</th>
<th>NB (AME)</th>
<th>OLS (coef.)</th>
<th>NB (AME)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Concentration</strong></td>
<td>-5.483**</td>
<td>-4.794**</td>
<td>-85.35**</td>
<td>-114.3***</td>
</tr>
<tr>
<td></td>
<td>(2.422)</td>
<td>(2.314)</td>
<td>(42.14)</td>
<td>(42.00)</td>
</tr>
</tbody>
</table>

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

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Observations</td>
<td>586</td>
<td>586</td>
<td>586</td>
<td>586</td>
</tr>
<tr>
<td>R-squared</td>
<td>0.388</td>
<td>0.386</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wald chi-squared</td>
<td>236.43</td>
<td></td>
<td>239.51</td>
<td></td>
</tr>
</tbody>
</table>

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*

<table>
<thead>
<tr>
<th></th>
<th>OLS (coef.)</th>
<th>OLS (IRR)</th>
<th>NB (coef.)</th>
<th>NB (IRR)</th>
<th>OLS (coef.)</th>
<th>OLS (IRR)</th>
<th>NB (coef.)</th>
<th>NB (IRR)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Concentration</strong></td>
<td>-5.361**</td>
<td>0.932**</td>
<td>-5.496**</td>
<td>0.924***</td>
<td>-5.850**</td>
<td>0.914***</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(2.552)</td>
<td>(0.0265)</td>
<td>(2.561)</td>
<td>(0.0263)</td>
<td>(2.602)</td>
<td>(0.0260)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Big_mshare</strong></td>
<td>42.45</td>
<td>5.939***</td>
<td>21.33</td>
<td>8.925***</td>
<td>34.01</td>
<td>22.02***</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(34.78)</td>
<td>(2.367)</td>
<td>(42.03)</td>
<td>(4.227)</td>
<td>(51.62)</td>
<td>(12.72)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Big_mshare</strong></td>
<td>8.942</td>
<td>1.298***</td>
<td>4.349</td>
<td>1.435***</td>
<td>6.998</td>
<td>1.738***</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>#Concentration</strong></td>
<td>(5.447)</td>
<td>(0.0847)</td>
<td>(7.376)</td>
<td>(0.123)</td>
<td>(9.489)</td>
<td>(0.190)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Vulnerability specific
Soft. and vendor specific
Disclosure effect
All control variables are included
Time effect variables

<table>
<thead>
<tr>
<th>Observations</th>
<th>586</th>
<th>586</th>
<th>586</th>
<th>586</th>
<th>586</th>
<th>586</th>
</tr>
</thead>
<tbody>
<tr>
<td>R-squared</td>
<td>0.394</td>
<td>0.388</td>
<td>0.389</td>
<td>0.389</td>
<td>0.389</td>
<td>0.389</td>
</tr>
<tr>
<td>Wald chi-squared</td>
<td>241.40</td>
<td>239.96</td>
<td>246.04</td>
<td>246.04</td>
<td>246.04</td>
<td>246.04</td>
</tr>
</tbody>
</table>

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

\[ \text{Big}_m\text{share} = 1 \text{ when the web browser’s market share is greater than 0.50} \]

\[ \text{Big}_m\text{share} = 1 \text{ when the market share is greater than 0.40} \]
Results (4/4): Impact of public disclosure of vulnerability information & open source component

<table>
<thead>
<tr>
<th>Concentration:</th>
<th>(-n)</th>
<th>(HHI)</th>
<th>(-n)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Big_mshare = 1:</td>
<td>(OLS)</td>
<td>(NB)</td>
<td>(OLS)</td>
</tr>
<tr>
<td>disclosure</td>
<td>-49.59***</td>
<td>-49.56***</td>
<td>-49.87***</td>
</tr>
<tr>
<td>open_source</td>
<td>-17.53***</td>
<td>-22.46***</td>
<td>-18.40***</td>
</tr>
</tbody>
</table>

All other variables are included except for vendor dummies.

Observations 586 586 586 586 586 586
R-squared 0.384 0.383 0.386 0.386 0.386 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.
1 Introduction
2 A model
3 Empirical strategy
4 Data
5 Results
6 Conclusion
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.


- No other theoretical or empirical studies on quality vs. competition of free products/software.
## Introduction

A model

Empirical strategy

Data

Results

Conclusion

Using as **Concentration**:

<p>| | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>-n</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OLS</td>
<td>NB</td>
<td>OLS</td>
<td>NB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Concentration</strong></td>
<td>-5.483**</td>
<td>-4.794**</td>
<td>-85.35**</td>
<td>-114.3***</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(2.422)</td>
<td>(2.314)</td>
<td>(42.14)</td>
<td>(42.00)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>vulnerability_severity</strong></td>
<td>-5.210**</td>
<td>-5.308**</td>
<td>-5.704***</td>
<td>-6.219**</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(2.050)</td>
<td>(2.567)</td>
<td>(2.188)</td>
<td>(2.593)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>vulnerability_type</strong> dummies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(10.65)</td>
<td>(10.50)</td>
<td>(10.63)</td>
<td>(10.46)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cwe704 (Incorrect type conversion or cast)</td>
<td>-8.606</td>
<td>-8.168</td>
<td>-7.544</td>
<td>-5.299</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(11.15)</td>
<td>(46.92)</td>
<td>(11.13)</td>
<td>(48.28)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>software_age</strong></td>
<td>0.755*</td>
<td>0.795</td>
<td>0.789*</td>
<td>0.798</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(0.438)</td>
<td>(0.530)</td>
<td>(0.442)</td>
<td>(0.527)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>apple</strong></td>
<td>-10.11</td>
<td>-13.92**</td>
<td>-11.54*</td>
<td>-14.95**</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(6.888)</td>
<td>(6.838)</td>
<td>(6.884)</td>
<td>(6.969)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>google</strong></td>
<td>-23.21*</td>
<td>-31.13***</td>
<td>-23.46*</td>
<td>-32.61***</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(12.16)</td>
<td>(46.92)</td>
<td>(12.01)</td>
<td>(48.28)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>mozilla</strong></td>
<td>-23.98***</td>
<td>-26.37***</td>
<td>-24.65***</td>
<td>-27.78***</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>disclosure</strong></td>
<td>-48.64***</td>
<td>-48.37***</td>
<td>-48.99***</td>
<td>-49.04***</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(3.611)</td>
<td>(4.462)</td>
<td>(3.631)</td>
<td>(4.474)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>qyear</strong></td>
<td>-1.513***</td>
<td>-1.513***</td>
<td>-1.605***</td>
<td>-2.276***</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(0.293)</td>
<td>(0.293)</td>
<td>(0.316)</td>
<td>(0.659)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Constant</strong></td>
<td>458.7***</td>
<td>549.1***</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(71.85)</td>
<td>(90.34)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Observations</td>
<td>586</td>
<td>586</td>
<td>586</td>
<td>586</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R-squared</td>
<td>0.388</td>
<td>0.386</td>
<td>0.386</td>
<td>0.386</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wald chi-squared</td>
<td>236.43</td>
<td>239.51</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VIF for <strong>Concentration</strong></td>
<td>1.40</td>
<td>1.68</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Robust standard errors in parentheses

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

The effect of competition intensity on software security

Telecom Paristech