Measuring Patching at Scale

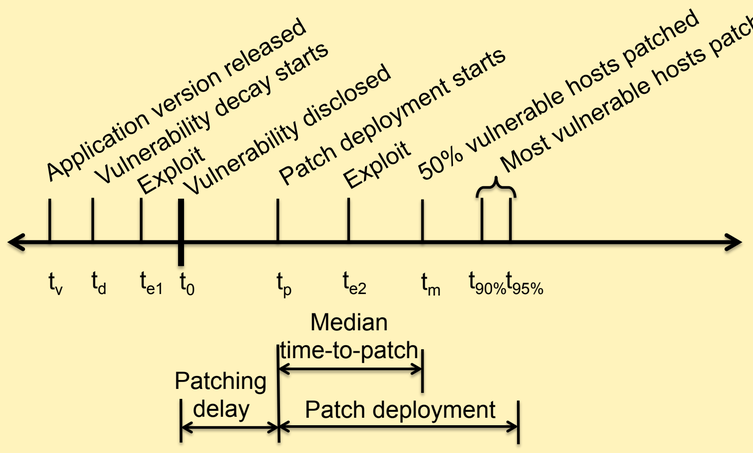
PI: Tudor Dumitraș, University of Maryland, College Park

http://www.umiacs.umd.edu/~tdumitra/research-patching-models.html

How do vulnerable host populations decay over time?

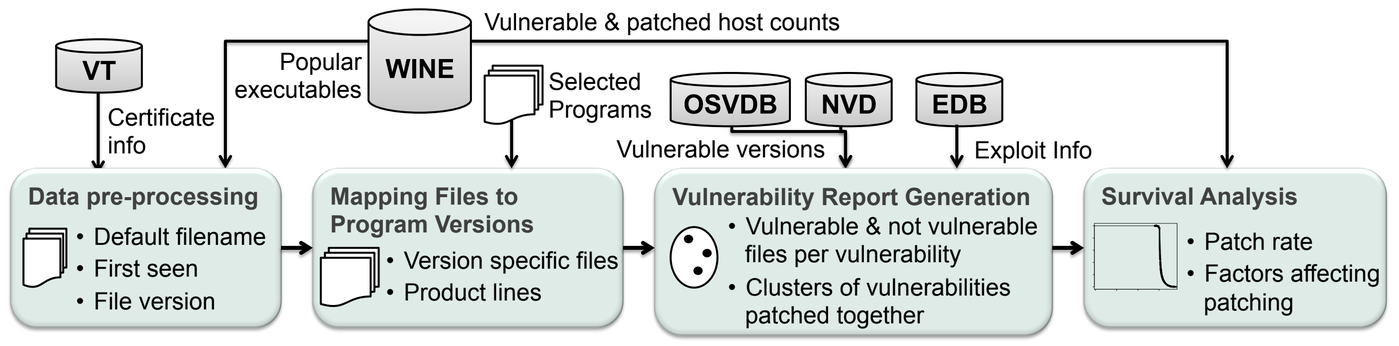
Vulnerabilities in **client applications** cannot be discovered by network scanners and are often exploited in spear-phishing attacks.

We aim to measure
- Patching rate
- Median time-to-patch
- Time to complete the patch deployment



Need to observe the patch deployment **on end-hosts** around the world.

Approach

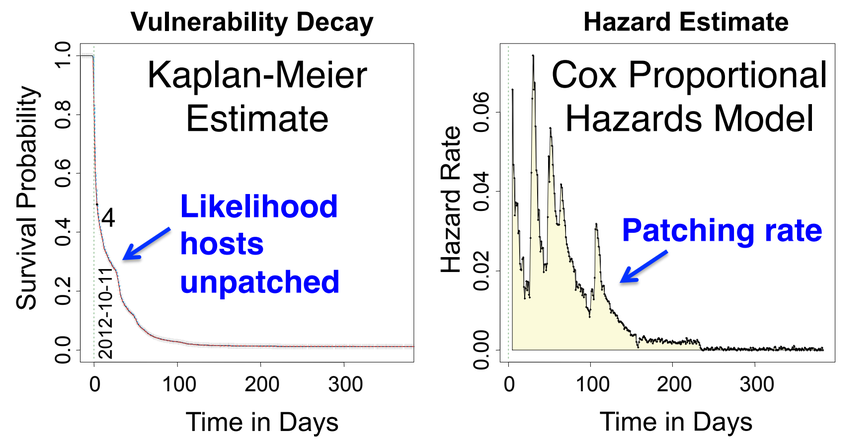


Datasets and Applications

Using WINE, we analyze the patch deployment for **1,593 vulnerabilities** in **10 client-side applications**:

- Email: Thunderbird
- Reader: Adobe Reader
- Editor: Microsoft Word
- Networking: Wireshark
- Multimedia: Flash Player, Quicktime
- Browsers: Chrome, Firefox, Opera, Safari

Survival Analysis



Patch Deployment

Milestones: Patch Deployment per Program

Program	Patch Delay	Days to patch (% clust.) t_m	Days to patch (% clust.) $t_{95\%}$	% Versions Auto
Chrome	-1	15 (100%)	447 (71%)	100.0%
Firefox	-5.5	36 (91%)	365 (24%)	2.7%
Flash	0	247 (59%)	1,002 (5%)	14.9%
Opera	0.5	228 (100%)	N/A (0%)	33.3%
Quicktime	1	268 (93%)	N/A (0%)	0.0%
Reader	0	188 (90%)	341 (13%)	12.3%
Safari	1	123 (100%)	934 (8%)	0.0%
Thunderbird	2	27 (94%)	159 (23%)	3.2%
Wireshark	4	N/A (0%)	N/A (0%)	0.0%
Word	0	79 (100%)	1,146 (33%)	37.4%

Negative patch delay indicates patching started before disclosure, zero indicates patching and advisory coordination. Chrome has the shortest t_m, followed by Thunderbird and Firefox, while Wireshark is the slowest and never reaches 50%.

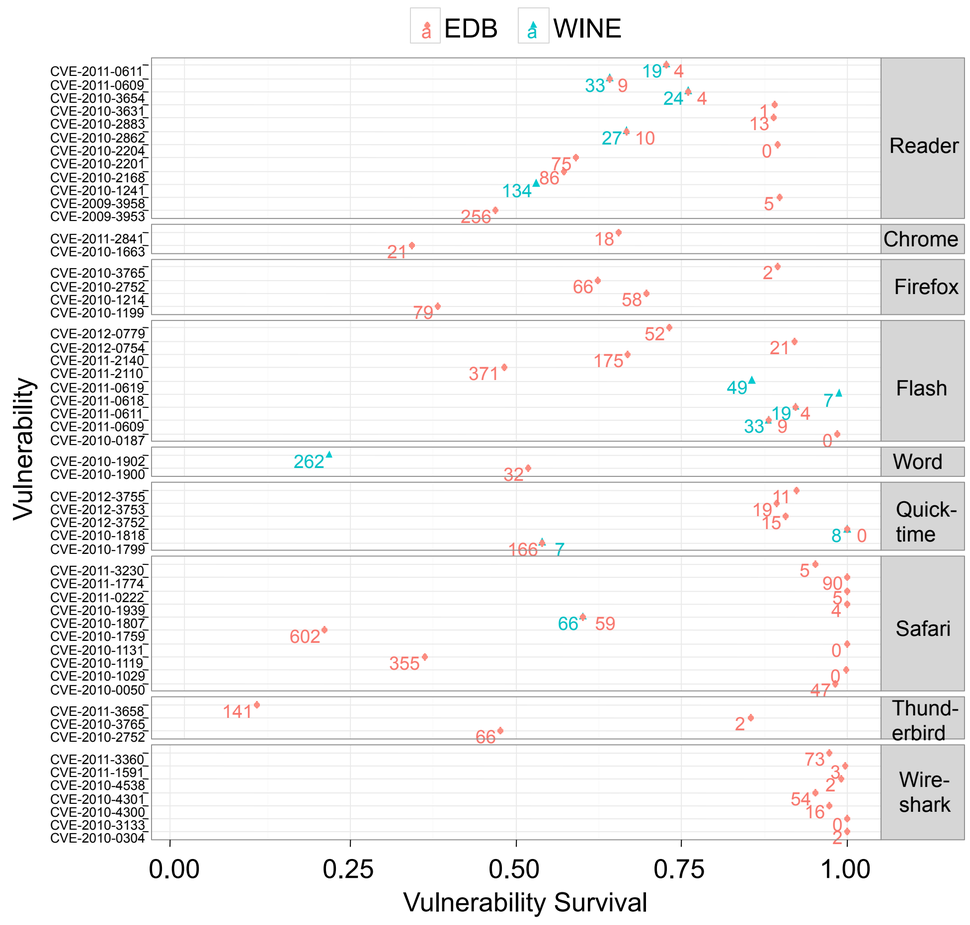
Factors Affecting the Patch Deployment

Categories	Median time-to-patch (% reached) All	Reader	Flash	Firefox
Professionals	30 (79%)	103 (90%)	201 (73%)	25 (92%)
Software Developers	24 (80%)	68 (90%)	114 (86%)	23 (90%)
Security Analyst	18 (93%)	27 (87%)	51 (91%)	13 (89%)
All users	45 (78%)	188 (90%)	247 (60%)	36 (91%)
Silent Updates	27 (78%)	62 (90%)	107 (86%)	20 (89%)
Manual Updates	41 (78%)	97 (90%)	158 (81%)	26 (88%)

Security analysts tend to patch faster than other user categories. Automated update mechanisms also lead to faster patching.

Vulnerable Population

What percentage of the host population is still vulnerable when exploits are created?



Median percentage of hosts patched: **14%**.

Only **one** real-world exploit found more than 50% of hosts patched.

These numbers should be interpreted as **upper bounds**.

Exploits are generally effective, **even if not zero-day**.

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Nov. 27 -29th 2012
National Harbor, MD

MARYLAND CYBERSECURITY CENTER