



# Web Browser Security Update Effectiveness

Talk at CRITIS 2009

Dr. Thomas Dübendorfer, Google

Dr. Stefan Frei, ETH Zürich

Contact: <http://www.techzoom.net/silent-updates>



# Critical Infrastructures

## The device:

- User Base: 1.4 billion
- Coverage: Global
- Type of usage: Private, Commercial, and Government, Military

➔ A critical infrastructure component?

We talk about Web Browsers.

- Highly exposed and heavily attacked target
- Free of vulnerabilities? Always patched?



# Systems are connected

## The problem:

1. Web Browsers have security vulnerabilities.
2. Web Browsers became the primary attack target.

➔ Internet users, their data and connected systems are at risk:

- Data theft, industry espionage
- Connected systems (e.g. control networks)
- Resource misuse (e.g. bot networks, spam)

# How many surf with outdated browsers?

**637 million (45%)** Internet users surf the Web without using the latest most secure Web Browser version available.

This is browsers with update mechanisms.

**How about your SCADA systems?**

**How do you update a remote controlled valve in a power plant?**

Reference:

„Understanding the Web Browser Threat”, S. Frei, T. Dübendorfer, July 2008.



# Update mechanisms are key

- Every software has vulnerabilities
- Networking exposes every device to attacks

As a consequence:

- Software update capabilities are critical
- Update must cover the entire device population

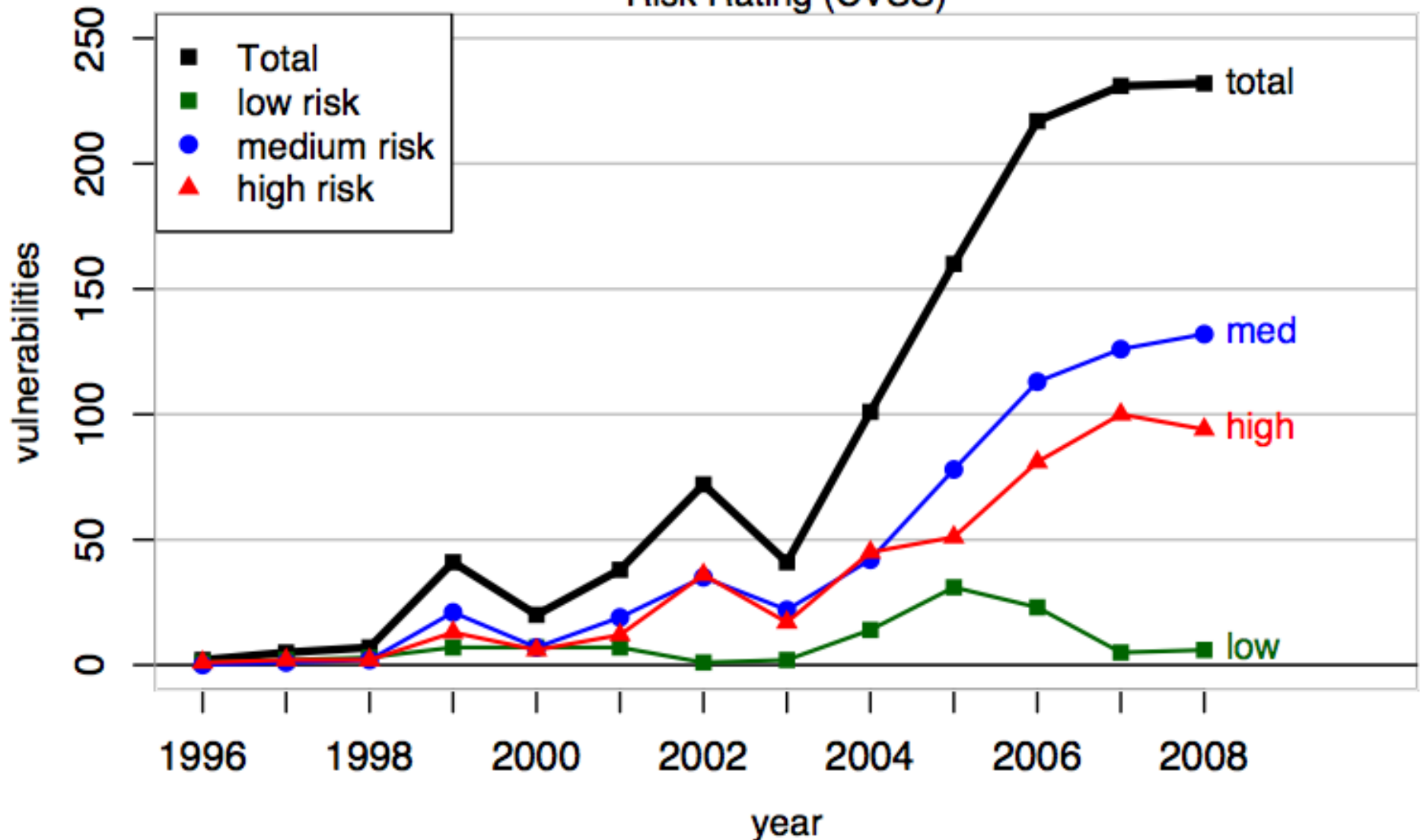
Our study: Effectiveness of different Web browser update mechanisms measured at global scale.

# Web Browser Security Vulnerabilities



# New Web Browser vulnerabilities / year

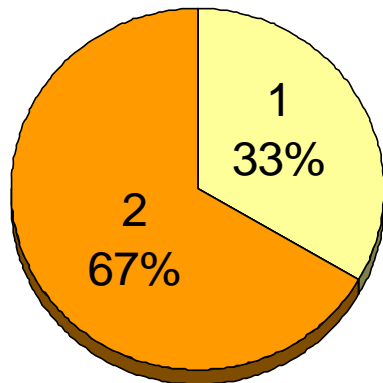
**Web Browser**  
Risk Rating (CVSS)



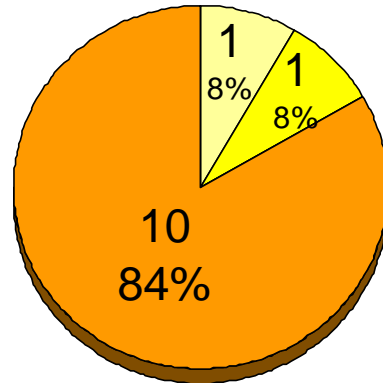
# Web Browser vulnerabilities by criticality

(Jan 1, 2009 – Sept 20, 2009)

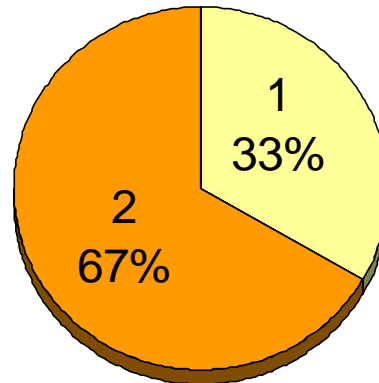
Microsoft  
IE 8.x



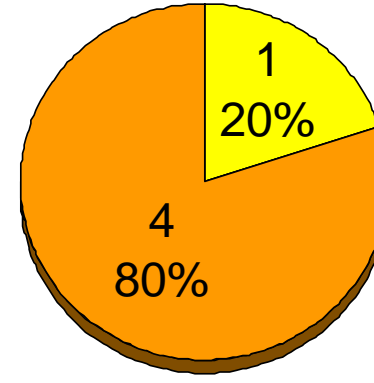
Mozilla  
Firefox 3.0.x



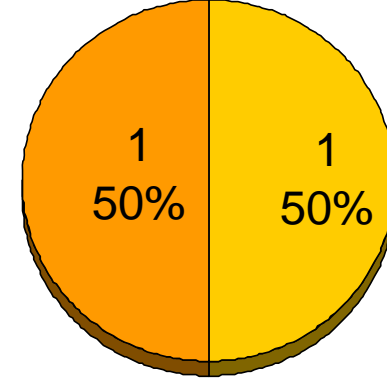
Apple  
Safari 4.x



Google  
Chrome 2.x



Opera  
Opera 9.x



- 1 (not critical)
- 2 (less critical)
- 3 (moderately critical)
- 4 (highly critical)
- 5 (extremely critical)

**In 2009, any major Web Browser had at least one remotely exploitable security bug that allowed for unauthorized system access. The same is true for 2008.**

Data source: Secunia, Sept 20th, 2009

# Drive-By Downloads



# Drive-By Download

A drive-by download is the act of **installing software** on a computer of a website visitor **without** getting prior **consent**.



Source: istockphoto

## Malware features:

- **Keylogger** (to steal information)
- **Trojans** (to misuse resources; remote control machine)
- **Anti-“malware removal“ tools** (to keep system infected)
- and more ...

# Attack vector (you can't hide)






The screenshot shows a Mozilla Firefox browser window displaying the DHS SBIR website. The address bar shows the URL <https://www.sbir.dhs.gov/index.aspx>. The page features a navigation menu on the left with items like 'SBIR Home', 'News and Events', 'Sollicitation Deadlines', 'Proposal Submission', 'SBIR Sollicitations', 'Awards', 'Awardee Portal', 'FAQ', 'Links', 'Topic Recommendations', 'Mailing List', 'Privacy Policy', 'SBIR Contact Information', and 'Site Search'. The main content area has a header for 'Homeland Security SBIR Program' and a central announcement: 'The DHS S&T SBIR FY09.2 sollicitation closed on July 2, 2009.' Below this is the title 'Department of Homeland Security Science and Technology Directorate (S & T Directorate) Small Business Innovation Research (SBIR) Program'. The main text describes the program's history and goals. A vertical stack of images on the right side of the page shows various scientific and technological activities. The browser's status bar at the bottom shows 'Done' and the website URL 'www.sbir.dhs.gov'.

April 2008, .ASP SQL injection attack/drive-by download

# The Solution: Web Browser Security Updates!



# Browser Update Discovery

	Browser	Discovery	Download	Installation (+Restart)
	Google Chrome	5 hrs	automatic	automatic no user action required
	Mozilla Firefox	start-up never	automatic never	manual one mouse click
	Apple Safari	daily never	(automatic) manual, never	manual
	Opera	weekly never	manual never	manual (new browser installation < v9)
	Microsoft IE	daily never	automatic never	automatic or manual

Legend: **High** and **low** update effectiveness settings.

# Global Web Browser measurement study

## Input:

Anonymized access logs of worldwide Google web servers:

- visit time
- cookie id per visit
- Web Browser HTTP user agent string  
(IE does not report minor version number in user agent string.)

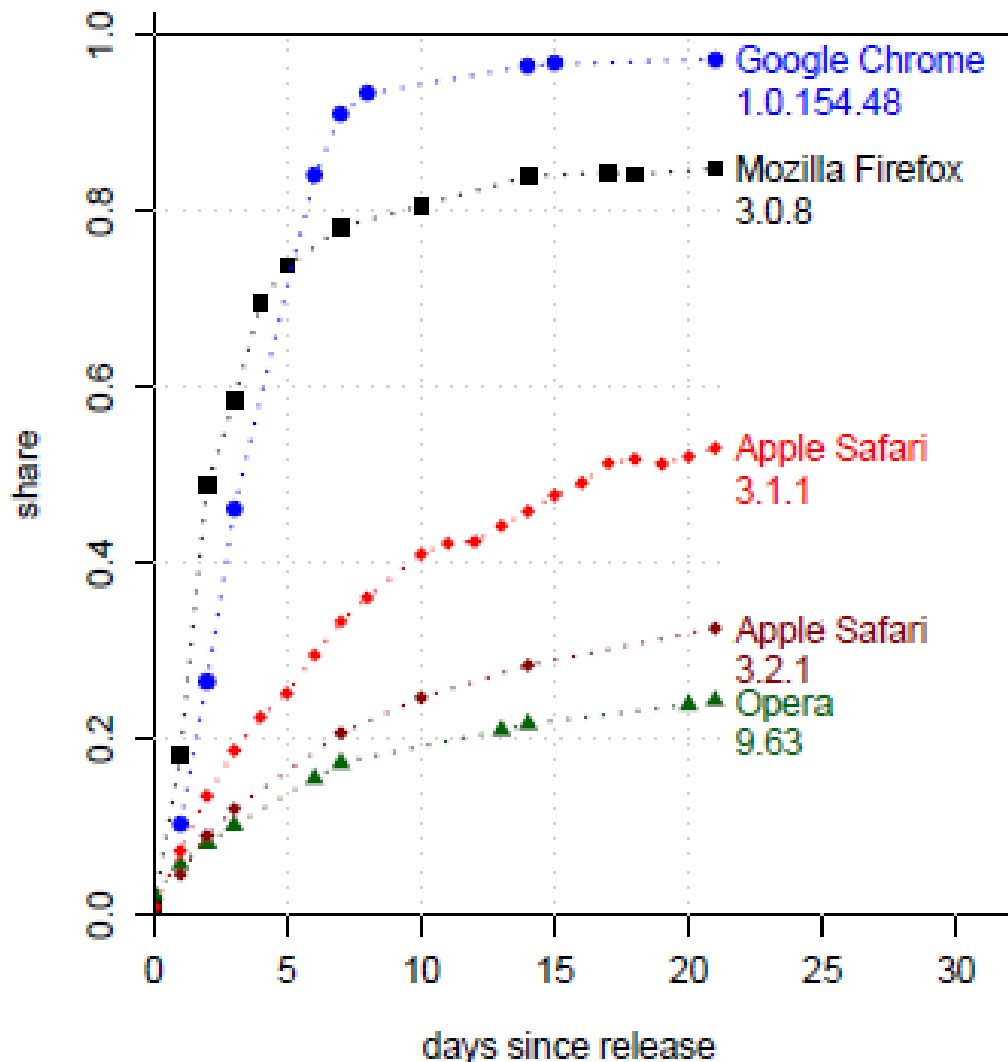
## Output:

Usage shares of browsers in active use per day by browser major (e.g. 3.x) and minor (e.g. 0.8) version and operating system.

Sample user agent string:

„Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.9.0.8)  
Gecko/2009032609 **Firefox/3.0.8**“

# Which Web Browser updates the fastest?



Three weeks after availability of a Web Browser update:

- 97% Google Chrome
- 85% Mozilla Firefox
- 53% Apple Safari
- 24% Opera

users are up-to-date.

Reference:

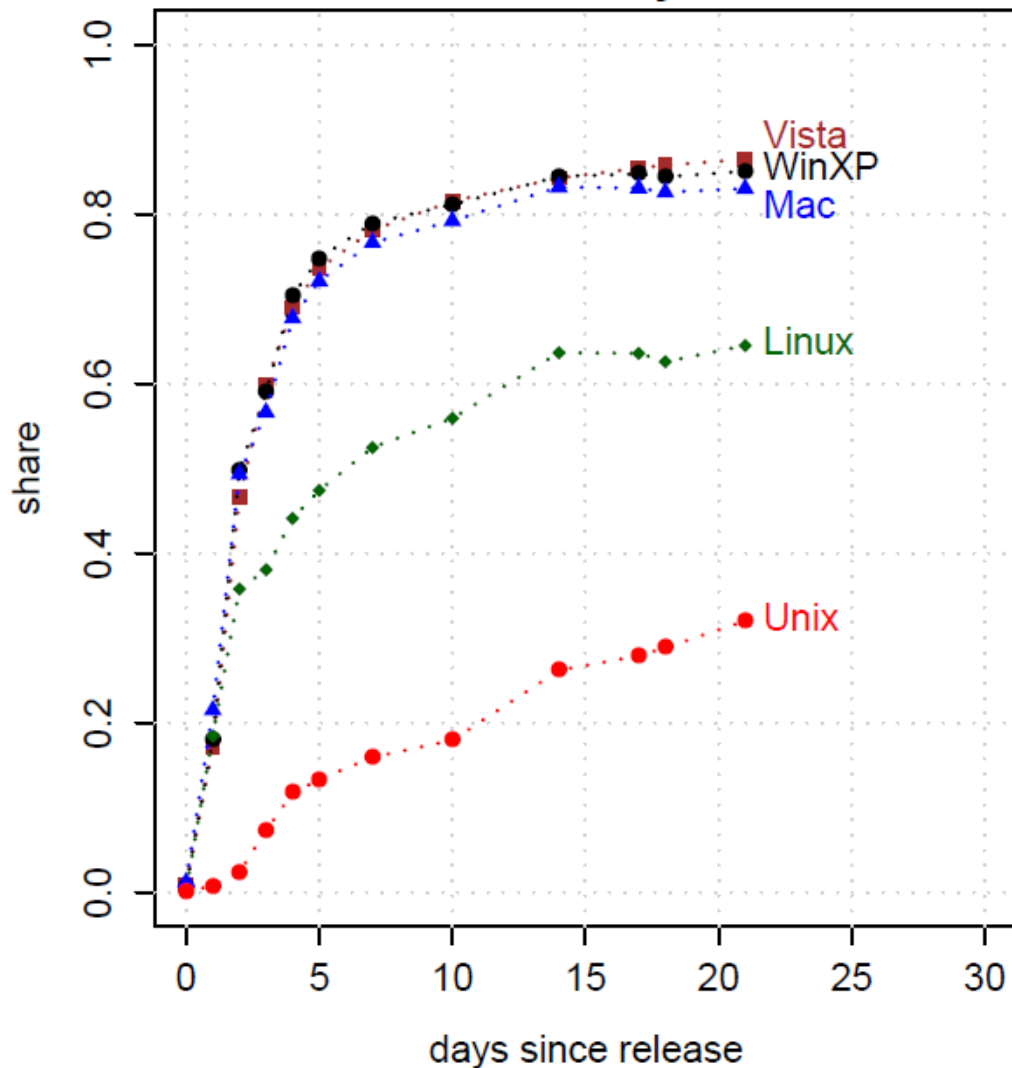
“Why Silent Updates Boost Security”, T. Dübendorfer, S. Frei, <http://www.techzoom.net/silent-updates>

# The Role of the Operating System

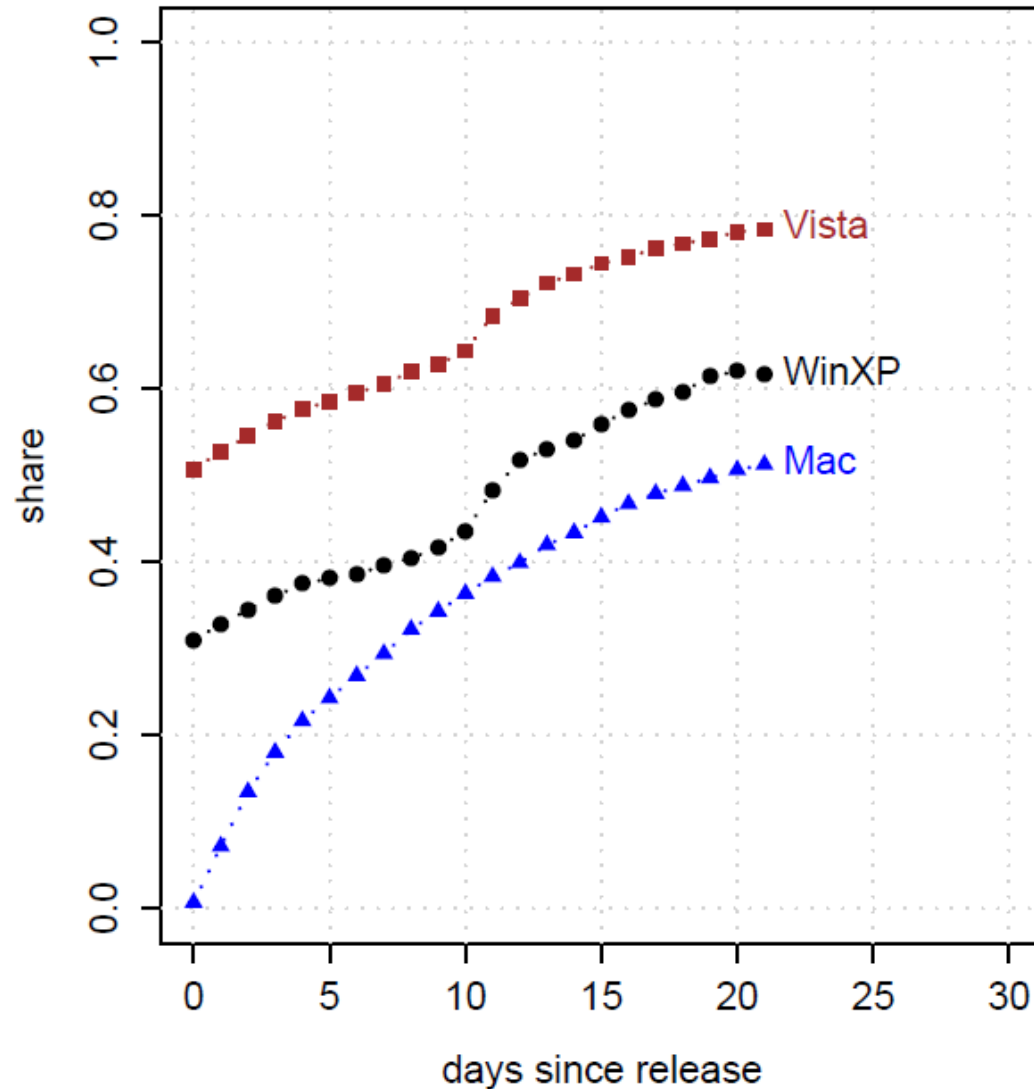


# Update effectiveness by operating system

## Firefox 3.0.8 dynamics



## Safari 3.1.2 dynamics



Reference: Research results by S. Frei, T. Dübendorfer, 2009

# Concluding Remarks



# Browser vs. SCADA attack targets

	<b>Browser</b>	<b>SCADA</b>
Target attractiveness	PII, Credit card System access	Own power plant Gas pipeline Beer brewery
Vulnerabilities	Yes	Yes
Update mechanism	Yes	?
Update discovery	Yes	?
Update installation	Yes	?
Update effectiveness	Measured; within days to months	?
Device lifetime	1-5 years	10-50 years

# Conclusion: Update mechanisms are key

- Every software has vulnerabilities
- Networking exposes every device to attacks

As a consequence:

- Software update capabilities are critical
  - Update must cover the entire device population
- 
- **How do you update your SCADA devices?  
Power meters etc.**

# References

Mentioned research papers are available for download at:

<http://www.techzoom.net/publications>

**Web Browser Security Update Effectiveness**, T. Dübendorfer [Google], S. Frei [ETH], Springer LNCS Proceedings of CRITIS 2009, Bonn, Oct. 2009

**Why Silent Updates Boost Security**, T. Dübendorfer [Google], S. Frei [ETH], ETH Tech Report TIK 302, May 2009

<http://www.techzoom.net/silent-updates>

**Firefox (In)security Update Dynamics Exposed**, S. Frei [ETH], T. Dübendorfer [Google], B. Plattner [ETH], [ACM SIGCOMM Computer Communication Review](#), January 2009

<http://www.techzoom.net/papers/>

[sigcomm\\_ccr\\_firefox\\_\(in\)security\\_update\\_dynamics\\_exposed.pdf](http://www.techzoom.net/papers/sigcomm_ccr_firefox_(in)security_update_dynamics_exposed.pdf)

**Understanding the Web Browser Threat: Examination of vulnerable online Web Browser populations and the "insecurity iceberg"**, S. Frei [ETH], T. Dübendorfer [Google], G. Ollmann [IBM ISS], M. May [ETH], [DefCon 16 2008](#), Aug 10, 2008, Las Vegas, USA; ETH Tech Report 288, July 2008

<http://www.techzoom.net/insecurity-iceberg>



**Thanks for your attention!**

**Speakers:**

**Dr. Thomas Dübendorfer, Google**

**Dr. Stefan Frei, ETH**

**[www.techzoom.net/silent-updates](http://www.techzoom.net/silent-updates)**