Ex-Ray: Detection of History-Leaking Browser Extensions

Michael Weissbacher
Northeastern University

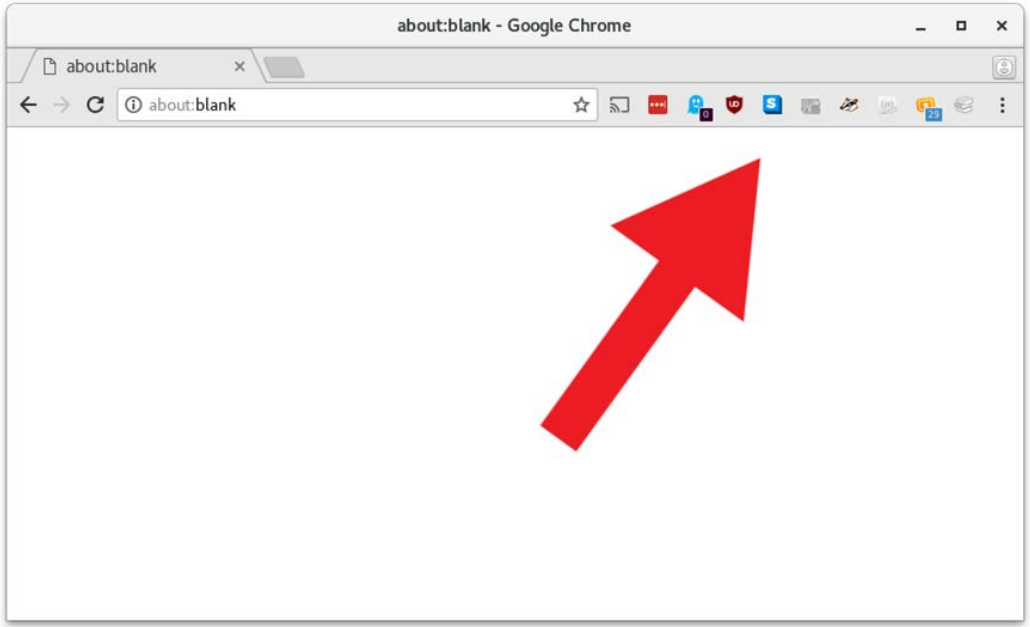
Joint work with:
Enrico Mariconti, Guillermo Suarez-Tangil,
Gianluca Stringhini, William Robertson, Engin Kirda

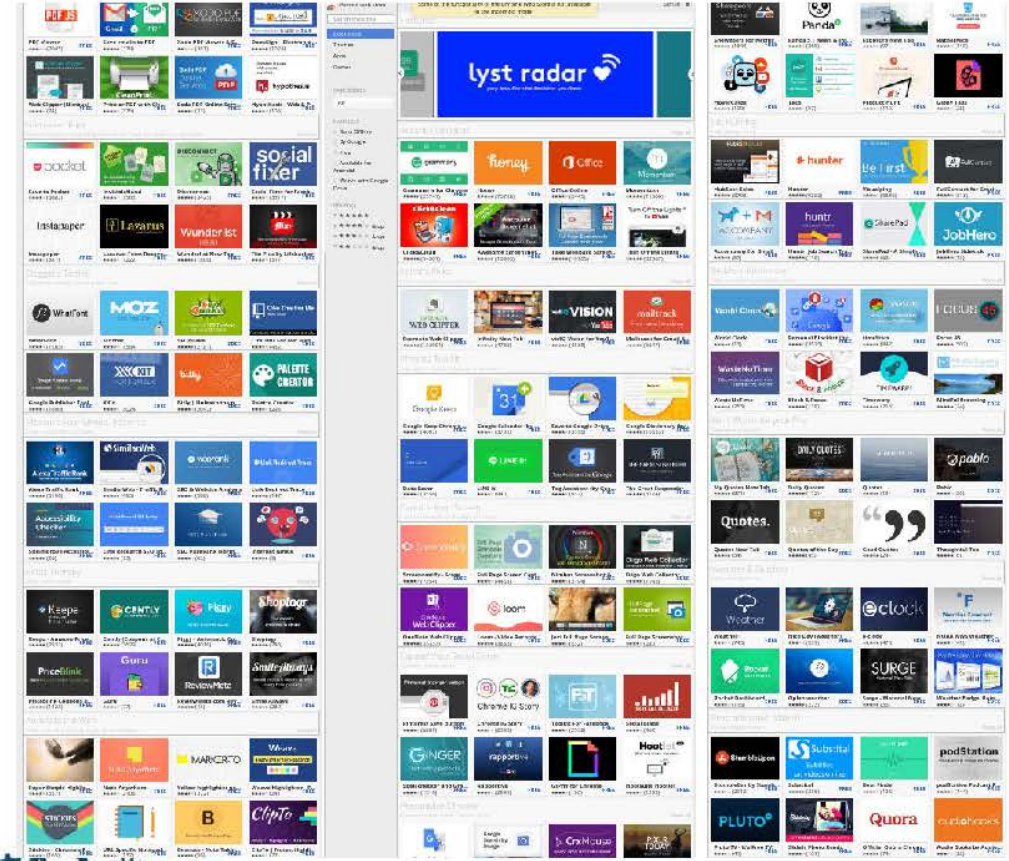
PRIVACYCON

What are Browser Extensions?

- Additions to browser core functionality
- Powerful application access based on permissions
  - Modification of active pages
  - Modification of requests / responses
  - Often access to all visited pages
  - Access to cookies
  - Access to previous history

What are Browser Extensions?




lyst radar
social fixer
Instapaper
Wunderlist
MOZ
PALETTE CREATOR
Quotes.
Quora
PLUTO

PRIVACYCON

Privacy Implications of Browser Extensions

- Permission system inadequate to contain history leaks
- Only modest permissions required to leak complete browsing history
- Collection sometimes mentioned in terms of service
- User expectation might not align with actual behavior
- Automatic updates of extensions can lead to future leaking behavior
- No unified way of detection or indication for users

Comparison Web Tracking and Extension Tracking

On Websites:

- Opt-in: Website owner
- Opt-out: Ad blockers or Tracker blockers

In Extensions:

- (typically) all websites
- Implicit Opt-in through installation
- No opt-out

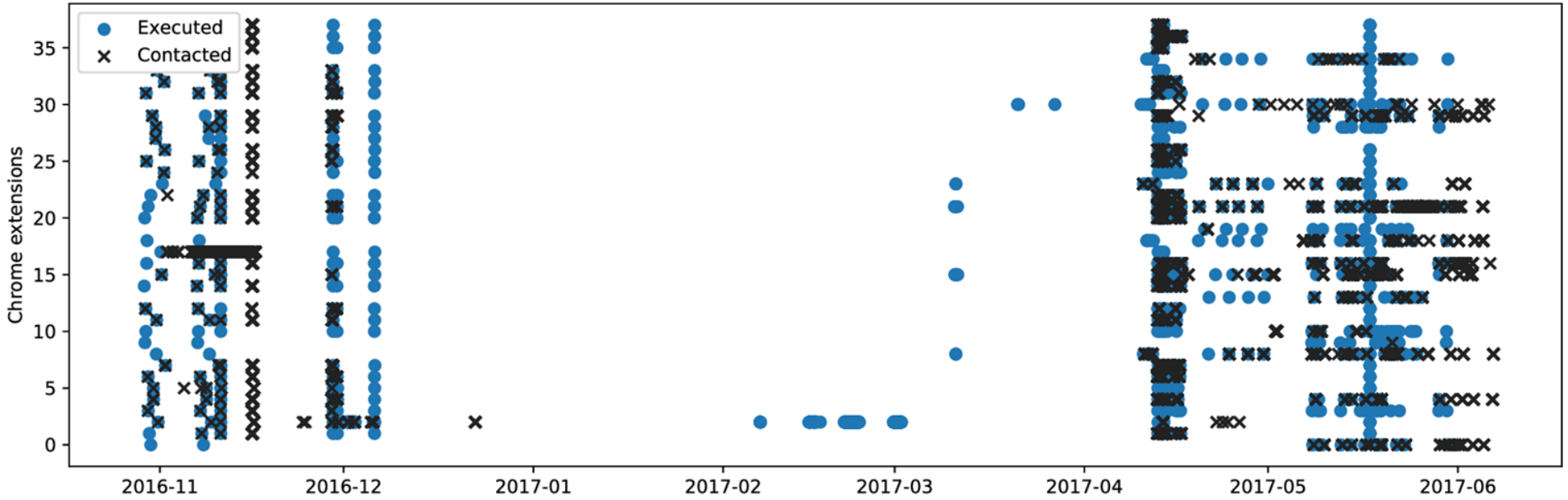
Motivation: Manual Analysis

- One library used across unrelated extensions to leak history
- 42 extensions
- 8M active users
- Findings documented in blog post
- Google deleted all extensions within 24 hours
- No change in policy

HoneyPot Probe: Overview

- Extensions run in isolation
- Use URLs unique to extension
- Browsing our website...
- ... which is also available on the public Internet
- Monitor for incoming connections

HoneyPot Probe



HoneyPot Probe: Results

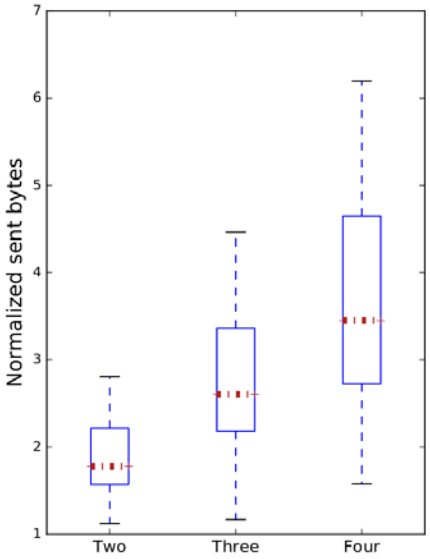
- Connections prove use of data: data is being acted on
- > 3M active users for these extensions
- Connection often immediately after execution
- Lower bound of leaks
- Indicators for collaboration
- Motivation for automated detection system

Ex-Ray: Overview

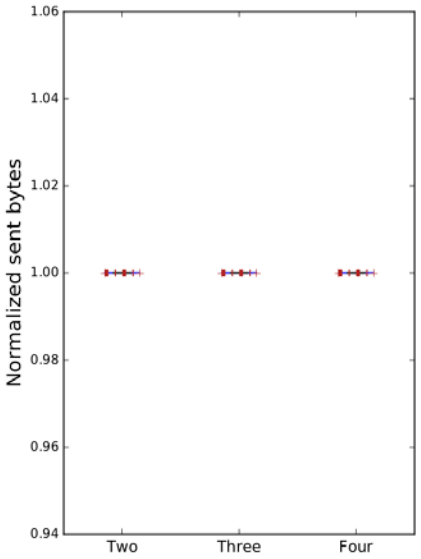
- System for automated detection of history leaks
- Goal: Robust Detection
  - Method of data collection
  - Traffic obfuscation / encryption
- Two complementary automated detection systems
- Additional triage system to assist analysts
- Based on Traffic analysis and browser instrumentation
- Analyzed extensions with more than 1,000 users (10,000+ extensions)

Ex-Ray: Methodology

- Counterfactual analysis
- Based on properties of tracking behavior
- Modifications to history lead to modified network behavior
- Sent data increases as a function of history size



(a) Tracking extension.



(b) Benign extensions.

Findings

- 10M+ active users were leaking their history
- 10,691 extensions analyzed
- 212 extensions flagged by Ex-Ray (28 wrongly identified - False Detection Rate: 0.27%)
- Two novel ways of leakage detected

Conclusion

- History leaks through browser extensions widespread
- Extension stores do not scan for history leaks
- Robust leak detection possible
- Possible remediation
  - Integration of leak detection into extension stores
  - Users should uninstall unused extensions

https://mweissbacher.com/blog/2017/10/05/ex-ray-finding-browser-extensions-that-spy-on-your-browsing-habits/