Hacking Google ChromeOS

Matt Johansen
Team Lead
matt.johansen@whitehatsec.com
@mattjay

Kyle Osborn
Application Security Specialist
kyle.osborn@whitehatsec.com
@theKos

August 2011

special thanks to:
Google’s Security Team
Jeremiah Grossman
Chris Evans
Who are we?

Kyle & Matt are both part of the Threat Research Center at WhiteHat Security and manually assess a large portion of WhiteHat’s 4,000+ websites.

• Matt:
  - Application Security Engineer turned Team Lead.
  - Background in Penetration Testing as a Consultant.
  - Bachelor of Science in Computer Science from Adelphi University

• Kyle:
  - Application Security Specialist
  - Primary focus on Offensive Security Research
  - Likes to push the Big Red Button
WhiteHat Security Company Overview

- WhiteHat Security: end-to-end solutions for Web security

- WhiteHat Sentinel: SaaS website vulnerability management
  
  *Combination of cloud technology platform and leading security experts turn security data into actionable insights for customers*

- Founded in 2001; Sentinel Premium Edition Service launched in 2003

- 400+ enterprise customers, 4,000 sites under management

- Most trusted brand in website security
Google Cr-48 Beta Laptop

- First Chrome OS dedicated device
- Application to be a Beta Tester open to public
- WhiteHat one of few security companies to test it first
Chrome OS

“The time for a Web OS is now” – Eric Schmidt

What we know:

• Revolves around the browser
• Virtually nothing stored locally
• Cloud heavy (re: reliant)
• Fast!
Chrome OS (cont’d)

Nothing stored locally = no usual software suspects.

**Mobile = App Crazy**

**Chrome OS = Extension Crazy**

In order to get usability / functionality out of a locked up device user’s must use what is available.
What Does A Hacker See?

New attack surface!

With all of these new extensions that aren’t necessarily developed by Google or any reputable company, security vulnerabilities are bound to be plentiful.

Let the Hacking Begin!
**ScratchPad**

**Preinstalled** note-taking extension

Auto Sync feature to Google Docs “ScratchPad” Folder

Google Docs “Feature” – Folder/Doc sharing. No permission needed!
ScratchPad Video demo

Google fixed Scratchpad XSS very quickly but we have a video demo.
Permission Structure

Why are Extensions any different?

- Individual extensions have unique permissions
- Use chrome.* API
- Permissions set by 3rd party developer
- Some extensions require permission to talk to every website
- Similar to Mobile Apps
Malicious Extension Demo

Saving this one for BlackHat.

What can we do with a very vulnerable extension with wide open permissions which do exist in the wild.
Browser -> Extension Trust Model

Taking the old Software Security Model and moving it to the cloud.

Software Security Model  Browser Extension Trust Model
Security Implications

“Chromebooks run the first consumer operating system designed from the ground up to defend against the ongoing threat of malware and viruses. They employ the principle of "defense in depth" to provide multiple layers of protection, including sandboxing, data encryption, and verified boot.”
– Google.com/Chromebook

Things Done Very Well
• Sandboxing tabs so they don’t talk to each other
• Local storage is virtually non existent
• Attack surface limited to client side browser exploits
• Handles own plugins (flash, pdfs, etc.)
• Eliminates most modern virus / malware threats
Thank You!

Q&A?

Matt Johansen  
Team Lead  
matt.johansen@whitehatsec.com  
@mattjay

Kyle Osborn  
Application Security Specialist  
kyle.osborn@whitehatsec.com  
@theKos