Move Fast Without Breaking Things

Kevin Parker
VP of WW Marketing … but don't be alarmed I'm still a geek at heart

SERENA

MOVE FAST AND BREAK THINGS

SERENA

Security

"…we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in a theft of intellectual property…"

"… at least twenty other large companies …"

Source http://googleblog.blogspot.com/2010/01/new-approach-to-china.html

Sources WSJ, TechWeb, MarketWatch, FT, Wired and others

SERENA

A clear and present danger

Clear and present and easy to discover

All Internet Service Licensees

Sub: Direction to block Internet Website.

Under the powers conferred by Section 69A of the Information Technology Ac
Technology (Procedures and Safeguards for Blocking of Access of Information by Public
to immediately block the access to the following 32 URLs:

1) https://justpaste.it/
2) http://hastebin.com
3) http://codepad.org
4) http://pastie.org
5) https://pastee.org
6) http://paste2.org
7) http://slexy.org
8) http://paste4btc.com/
9) http://0bin.net
10) http://www.heypasteit.com
11) http://sourceforge.net/projects/phorkie
12) http://atnsoft.com/textpaster
13) https://archive.org
14) http://www.hpage.com
15) http://www.ipage.com/
16) http://www.webs.com/
17) http://www.weebly.com/
18) http://www.000webhost.com/
19) https://www.freehosting.com
20) https://vimeo.com/
21) http://www.dailymotion.com/
22) http://pastebin.com
23) https://gist.github.com
24) http://www.ipaste.eu
25) https://thesnippetapp.com
26) https://snipt.net
27) http://tny.cz (Tinypaste)
28) https://github.com (gist-it)
29) http://snipplr.com/
30) http://term.ie.com
31) http://www.snippetsource.net
32) https://cryptbin.com

Source Forge

GitHub

Egor Homakov

Security consulting: Sakurity Twitter: @homakov. Subscribe to our new blog!

Friday, February 7, 2014

How I hacked Github again.

This is a story about 5 Low-Severity bugs I pulled together to create a simple giving me access to private repositories on Github.

These vulnerabilities were reported privately and fixed in timely fashion. H emails.

More detailed/alternative explanation.

Gotcha!
Github token with repo access?
Account takeover on gist
Hijack account on speakerdeck with oauth
OAuth redirect_uri issue

A few days ago Github launched a Bounty program which was a good motivator for me to play with Github OAuth.

Bug 1. Bypass of redirect_uri validation with /../

First thing I noticed was:

> If provided, the redirect URL's host and port must exactly match the callback URL. The redirect URL's path **must reference a subdirectory of the callb URL**

I then tried path traversal with /../ — it worked.

Bug 2. Lack of redirect_uri validation on get-tc endpoint

The first bug alone isn't worth much. There's protection in OAuth2 from "leaky" re 'code' has corresponding 'redirect_uri' it was issued for. To get an access token

PRANESH PRAKASH

DATA CENTER SOFTWARE NETWORKS SECURITY BUSINESS HARDWARE SCIENCE BOOTNOTES

The Register
Biting the hand that feeds IT

Git thee behind me, Git crit security bug!

Update anything on the desktop that touches GitHub if you want to live

19 Dec 2014 at 08:29, Simon Sharwood

127 25 14

GitHub has acknowledged there's a flaw in its client software and recommended that users upgrade as soon as possible.

News of the flaw was announced at GM/ issued a recommendation for "all users c soon as possible."

The flaw means " An attacker can craft a .git/config file when cloning or che the client machine."

www.bbc.com/news/technology-31729305

China and US clash over software backdoor proposals

President Obama said China should not be allowed to "snoop" on US tech firms' clients

GETTY IMAGES

Beijing has rejected President Obama's criticism of its plan to make tech companies put backdoors in their software and share their encryption keys if they want to operate in China.

On Monday, Mr Obama **told the Reuters news agency** he had "made it very clear" China had to change its policy if it wanted to do business with the US.

But Beijing said it needed the powers to combat terrorism and tackle leaks.

It also suggested the West was guilty of having double standards.

"The legislation is China's domestic affair, and we hop take a right, sober and objective view toward **ministry** spokeswoman Hua Chu

Related Stories

Sim card firm confirms hack attacks
US and UK 'hacked Sim card firm'
GCHQ v tech firms: Internet read

Sprawl

Mobility – Then and Now

£32.95
3.5 ounces
9 LEDs
36-byte memory
4 books of applications
No recorded cyber attacks

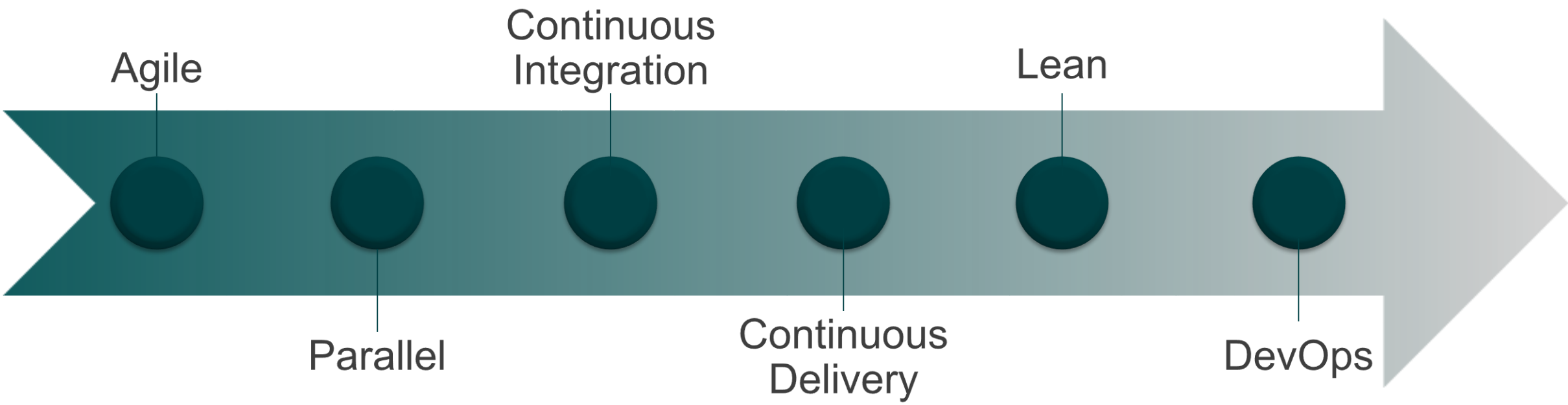
$699.00
4.5 ounces
1334x750 pixel display
128-gigabyte memory
1.2 million applications
1.6m Google hits for iPhone cyber attack

SERENA


Highly
Regulated
Large
Enterprises
Time-to-Market
Performance
Compliance
Risk
Move Fast Without Breaking Things


MOVE
FAST WITH
STABLE
INFRA

Modern Development Practices



Compliance

Performance

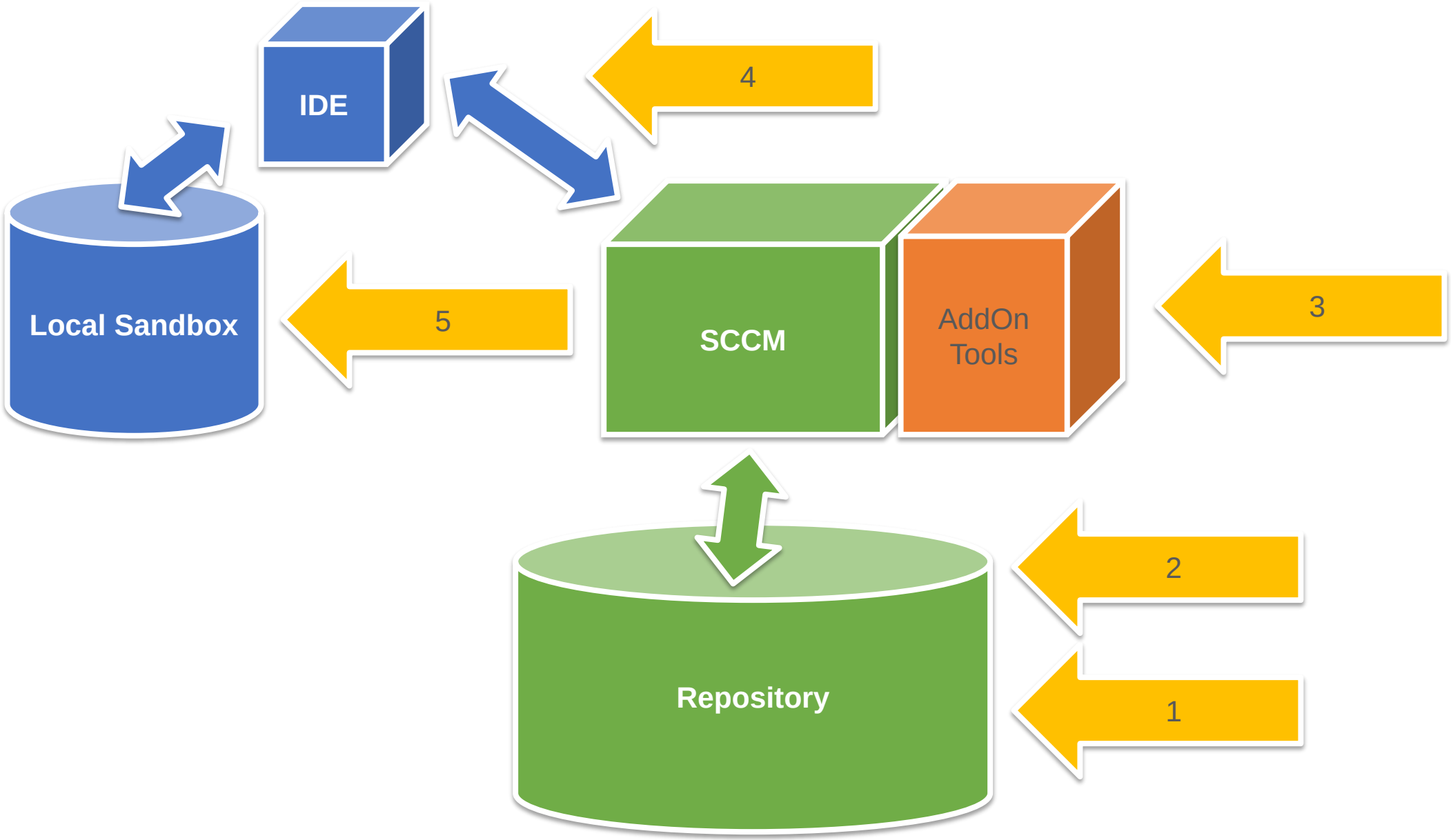
Modern Infrastructure

Typical Weaknesses

- Repository proliferation
- Policy enforcement
- Secure access control
- Process control
- Manual workflows
- Segregation of duties
- Traceability/audit support
- Compliance

git

SERENA


IDE
4
Local Sandbox
5
SCCM
AddOn
Tools
3
2
Repository
1

Five Best Practices

1. Adopt developer friendly tools

2. Upgrade process control in the SDLC

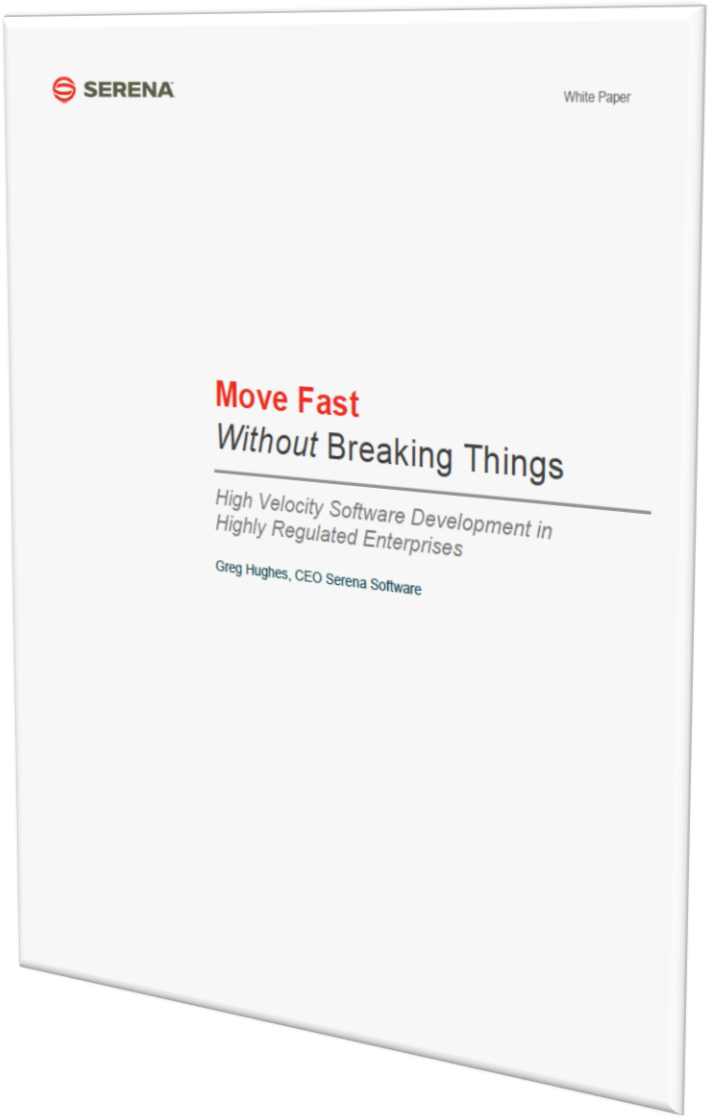
3. Automate wherever possible

4. Create centralized hardened SCCM

5. Use secure system for all app development

SERENA

Move Fast Without Breaking Things



SERENA