Postcards From a Post-Breach World

Jon Oberheide
CTO, Duo Security
jono@duosecurity.com

* title credit to lcamtuf
Hacking the Planet

Co-Founder & CTO

PhD Researcher

Talking to you!
ANDROID MARKET XSS BUG ALLOWED CODE EXECUTION ON MOBILE DEVICES

23 JUNE 2010

Exercising Our Remote Application Removal Feature

[This post is by Rich Cannings, Android Security Lead. — Tim Bray]

Duo Labs / Feb 25, 2013

Bypassing Google's Two-Factor Authentication

RESEARCHERS FIND METHODS FOR BYPASSING GOOGLE'S BOUNCER ANDROID SECURITY
Vision: Access
No "Perimeter"
Authentication
Authorization
Encryption
The real Duo...

Duo protects organizations by verifying the identity of the users and the health of the devices before connecting to the applications they need.

- Secure access
  - Trusted users
  - Trusted devices
  - Every application

- Quick stats
  - Founded in 2009
  - 6,000 customers
  - 72 NPS
  - ~300 FTEs
Duo + Google

- **Past**
  - Gnubby / U2F
  - ATAP Trust Anchor
  - Beyond Corp / nassh

- **Active**
  - Android SafetyNet / Verified Boot
  - CrOS Verified Access
  - Sesame API
  - Project “Keep bothering Juan to get the gnubby ssh-agent applet”
Today’s talk

- The present
  - Struggling with fundamental security problems
  - Breaches galore, of course
- The not-too-distant future
  - Cybercrime ROI diminishes
  - Inflection point of breaches
- The post-breach landscape
  - What happens after?
  - Note to self: swordsmithing lessons from Niels
Where are we today?
Buzzword bingo: de-perimeterization!

IT 1.0: Mainframe  IT 2.0: Client/Server  IT 3.0: Cloud/Mobile
Loss of traditional security controls

A loss of control precludes the deployment of most traditional security controls in an IT 3.0 environment.
Targeting end users

95% of breaches involve compromised credentials

75% of breaches involve compromised devices

Attackers are hijacking user access.
Focusing on the fundamentals

Where many organizations focus

- Detection and response
- Prevention
- An integrated portfolio that enables orchestration
- A focus on the fundamentals
- A dedication to recruiting and retaining staff
- An actual security strategy

Where we should focus
Security at its core is about reducing attack surface. You cover 90% of the job just by focussing on that. The other 10% is mostly luck.
Eric Schmidt’s advice to Obama

- Strong Authentication
- Up-to-Date Devices
- Encryption
Haven’t quite nailed those…

CIA director hack by teen spotlights US cyber-frailty

*John Brennan's compromised email demonstrates how even hi-tech superpowers can be bested by unsophisticated hackers.*

Lacking strong user auth  

Pictured: Flash and Java
75% of OS X devices out of date

71% of Android devices out of date

50% of iOS devices out of date

Android < 5.5.1, or < 6.0.1
OS X < 10.11.2
iOS < 9.2

<table>
<thead>
<tr>
<th></th>
<th>Nexus Phones</th>
<th>Other Android Phones</th>
</tr>
</thead>
<tbody>
<tr>
<td>Able to Receive Monthly Security Updates</td>
<td>99%</td>
<td>86%</td>
</tr>
<tr>
<td>Applied Latest Security Patch Level</td>
<td>66%</td>
<td>18%</td>
</tr>
<tr>
<td>Running Latest OS</td>
<td>87%</td>
<td>31%</td>
</tr>
</tbody>
</table>
Hackers Using Victim’s Own Software to Breach Network,…

Sophisticated attackers increasingly use little or no malware to compromise and steal data from their targets, according to an alert posted by managed security services firm Dell Secureworks on Sept. 2.

to conduct their intrusions. In this case, the threat actors used compromised credentials to log into an Internet-facing Citrix server to gain access to the network. CTU researchers discovered evidence that the threat actors were not only leveraging the company’s remote access infrastructure, but were also using the company’s endpoint management platform, Altiris, to move laterally through the network (see Figure 1).
Today's mega-dose of irony: endpoint security products that require you to install Java, Flash, Silverlight.
Release the Tavis!
How do we get to a better place?
Progress in the face of breaches
Who’s making it better?

RSA Conference vs Google, Microsoft, and Apple
User authentication

PAST

PRESENT

FUTURE
User authentication

- Properties of strong user auth
  - Credential security
  - User presence

- Primitives
  - Trusted compute/storage
  - Trusted input
  - Trusted display
Push/Prompt

- Easier than OTP
- OOB, mutual TLS
- Asym key in TEE
- Approval in REE
U2F with YK4s

- “Unphishable”
- Easier than Push/Prompt
- Limited by hardware form factor, cost, deployment
Ideal state for user auth

- Mobile device as root of trust
  - BTLE/NFC interfaces
- U2F/UAF credential in TEE
  - “Hardware-backed”
  - Built in to Android/iOS/Win10
- Unlock via biometric/KBA
  - Sesame for usability
  - Or TI/TD authz prompt
Hardware-backed security

“Hardware-backed” security = software written by hardware vendor = crappy software

http://bits-please.blogspot.com/
Device security

PAST

Windows XP

PRESENT

iOS

FUTURE

Windows 10

Diagram showing device security evolution from past to present to future.
CrOS

Security built-in

Seamless, automatic updates
Sandboxing
User separation/ encryption
Verified boot
Remote health attestation

CrOS Verified Access
From bolt-on to built-in

“The future is already here, it's just not very evenly distributed.” -- Gibson
Data @ Duo

- CrOS adoption
  - Hundreds of devices
- Windows 10
  - 15% of Win population
- U2F adoption
  - 1-2% of auths
- Ok, so it’s very unevenly distributed!
Tying these primitives into secure access and policy
Hard open problems

- Account recovery, credential bootstrapping
  - Ha!
- OAuth authz, scoping, phishing
  - Even easier than credential phishing
  - Pokemon Go, yay!
- Deep platform security
  - Firmware, AMT/ME, Ring -42
  - Joanna’s hypothetical stateless laptop
What happens after?
Tipping point

- Fundamentals become part of the platform
- Compromise becomes costly
- ROI declines for mass-market attackers
- Mass-market breaches decline
- Security problems become specialized for HVTs
Security industry

Gartner declares IDS obsolete by 2005

by Michael Mimoso
TechTarget
Published: 12 Jun 2003

Gartner Inc. is predicting that intrusion-detection systems will be obsolete soon, and recommends enterprises migrate to firewalls that block attacks rather than alert.

'The antivirus is dead? If you think that's news, you've been living in a different world'

Summary: With the continuing rise of cloud services, security execs have been proclaiming the death of antivirus software. But, according to F-Secure, the security is not so much dead as changed beyond all recognition.
Security technology

- AV/HIDS
- FW/IDS/IPS
- DLP
- WAF
- SIM/SEM
- DB/DAM
- Data protection
# Risky business

<table>
<thead>
<tr>
<th>Network Security</th>
<th>Firewall / VPN</th>
<th>Unified Threat Management</th>
<th>Intrusion Detection / Prevention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Security / Fraud Protection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Endpoint Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Messaging / Encryption</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Protection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security and Vulnerability Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability Assessment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity and Access Management</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
How far is the “future”?

Device security

● 1 year: Browser plugins eliminated
● 2-3 years: Remote health attestation for devices goes mainstream
● 3-5 years: Modern platforms will be prohibitively expensive to compromise to make mass-scale attacks worthwhile

User authentication

● 1 year: U2F gains mainstream adoption with BTLE/NFC/mobile interfaces
● 2-3 years: Universal unphishable hardware-backed authentication built in to all new mobile devices
● 3-5 years: Passwords eliminated
Microsoft Says Windows 10 Runs 350 Million Devices

For the first time, Google beat Apple in PC sales — and that's really bad news for Microsoft

by Dina Bass

Got a smartphone? FIDO and Bluetooth SIG want to use it for online authentication

Why carry a dedicated USB key to prove your online identity when your Bluetooth-enabled smartphone can do it for you?

Passport name out, Hello anchors Windows 10 MFA platform

Windows 10 Anniversary Update showcases evolution of Microsoft’s multi-factor authentication efforts

By John Fontana for Identity Matters | June 29, 2016 -- 22:05 GMT (15:05 PDT) | Topic: Microsoft

Web Authentication Working Group Charter

The mission of the Web Authentication Working Group, in the Security Activity, is to define a client-side A

Join the Web Authentication Working Group.
Legacy is the biggest thing holding organizations back.
What should Google do?
What should Google do?

- 5-year secure access roadmap
  - Expand beyond user auth: users, devices, access
  - Keep pushing BeyondCorp story, legacy migration

- Start the FIDO for devices
  - Verified boot, remote attestation, TEEs, etc
  - Ivan’s Bitfrost, cpalmer’s blog, etc

- Focus on the enterprise
  - You have the tech, need the GTM
  - MSFT is running the table...
Thanks!

Q&A

jono@duo.com