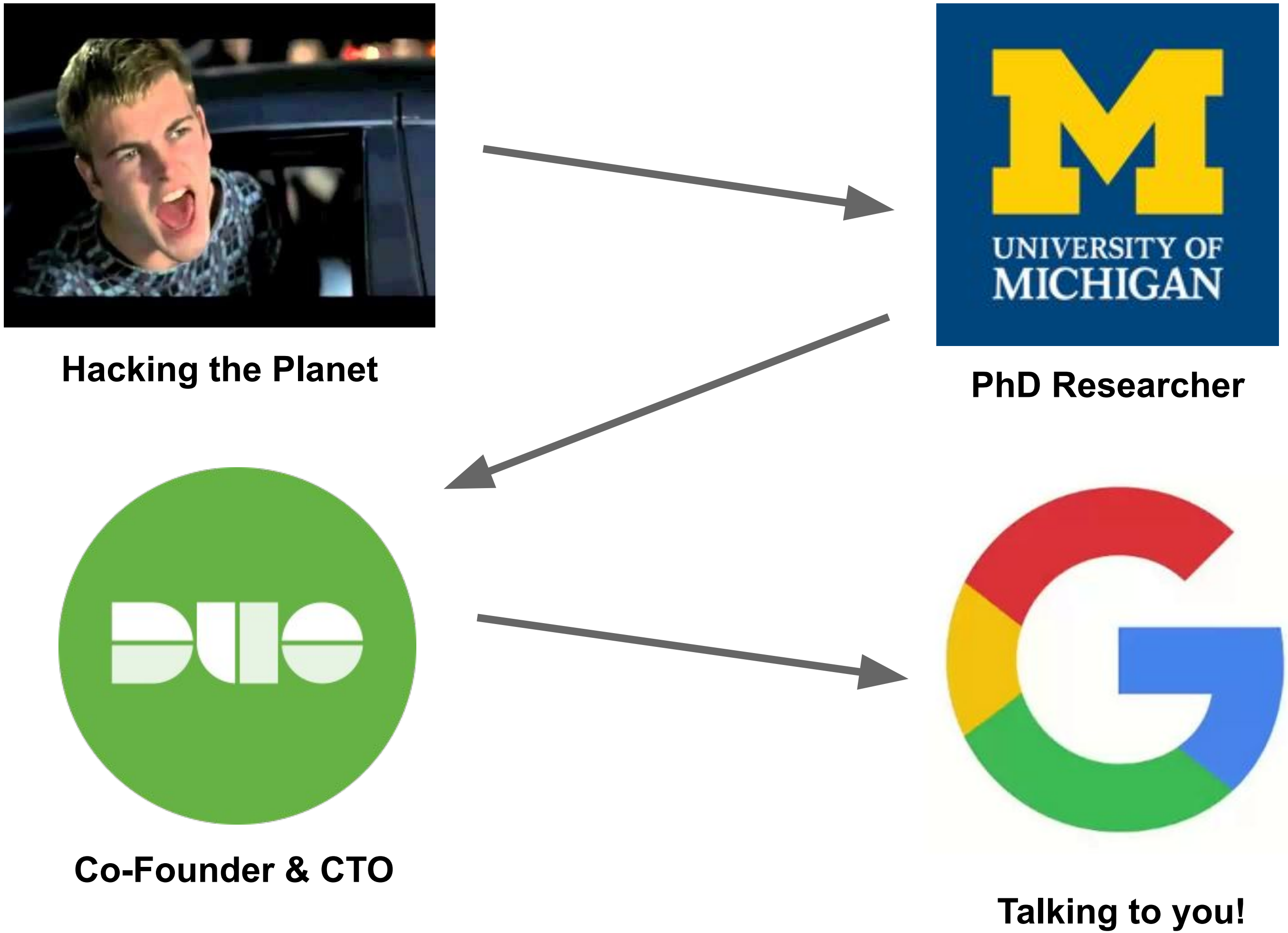
Postcards From a Post-Breach World

Jon Oberheide

CTO, Duo Security
jono@duosecurity.com

* title credit to lcamtuf

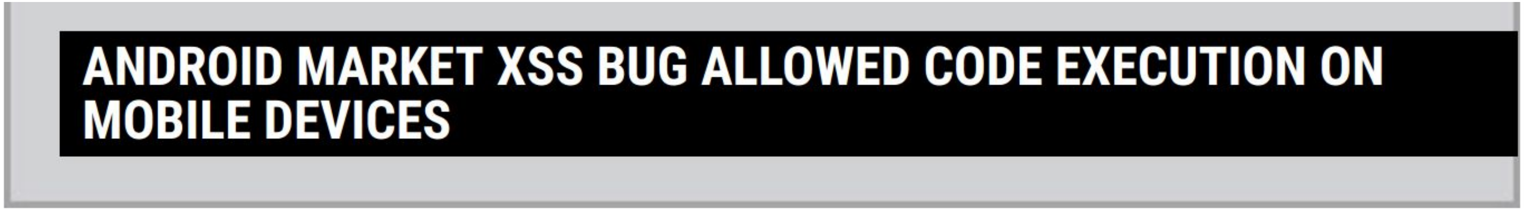


Hacking the Planet

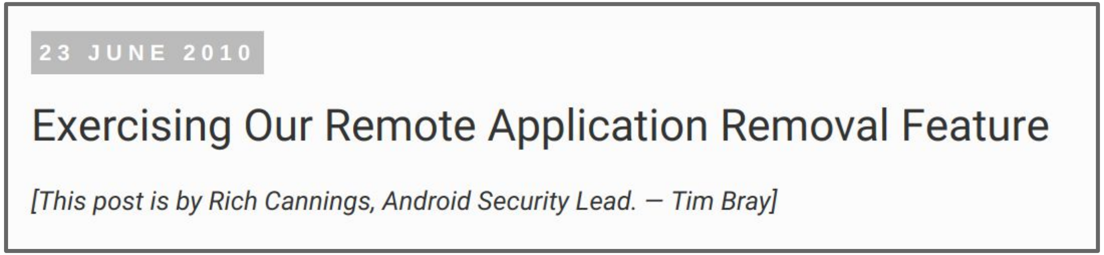
PhD Researcher

Co-Founder & CTO

Talking to you!



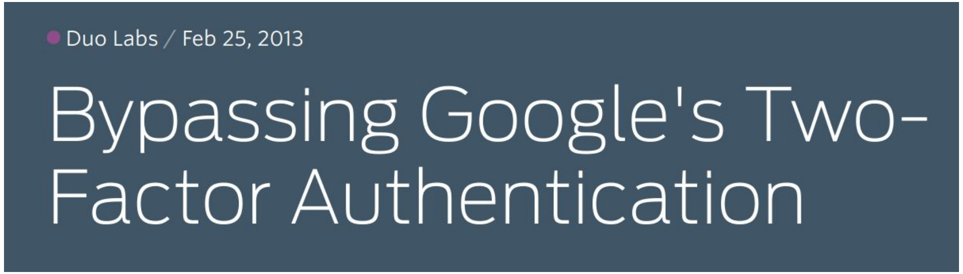
ANDROID MARKET XSS BUG ALLOWED CODE EXECUTION ON MOBILE DEVICES



23 JUNE 2010

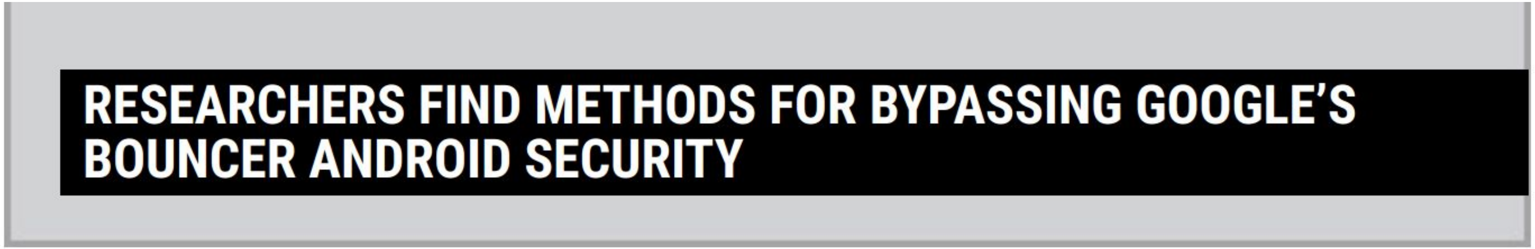
Exercising Our Remote Application Removal Feature

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

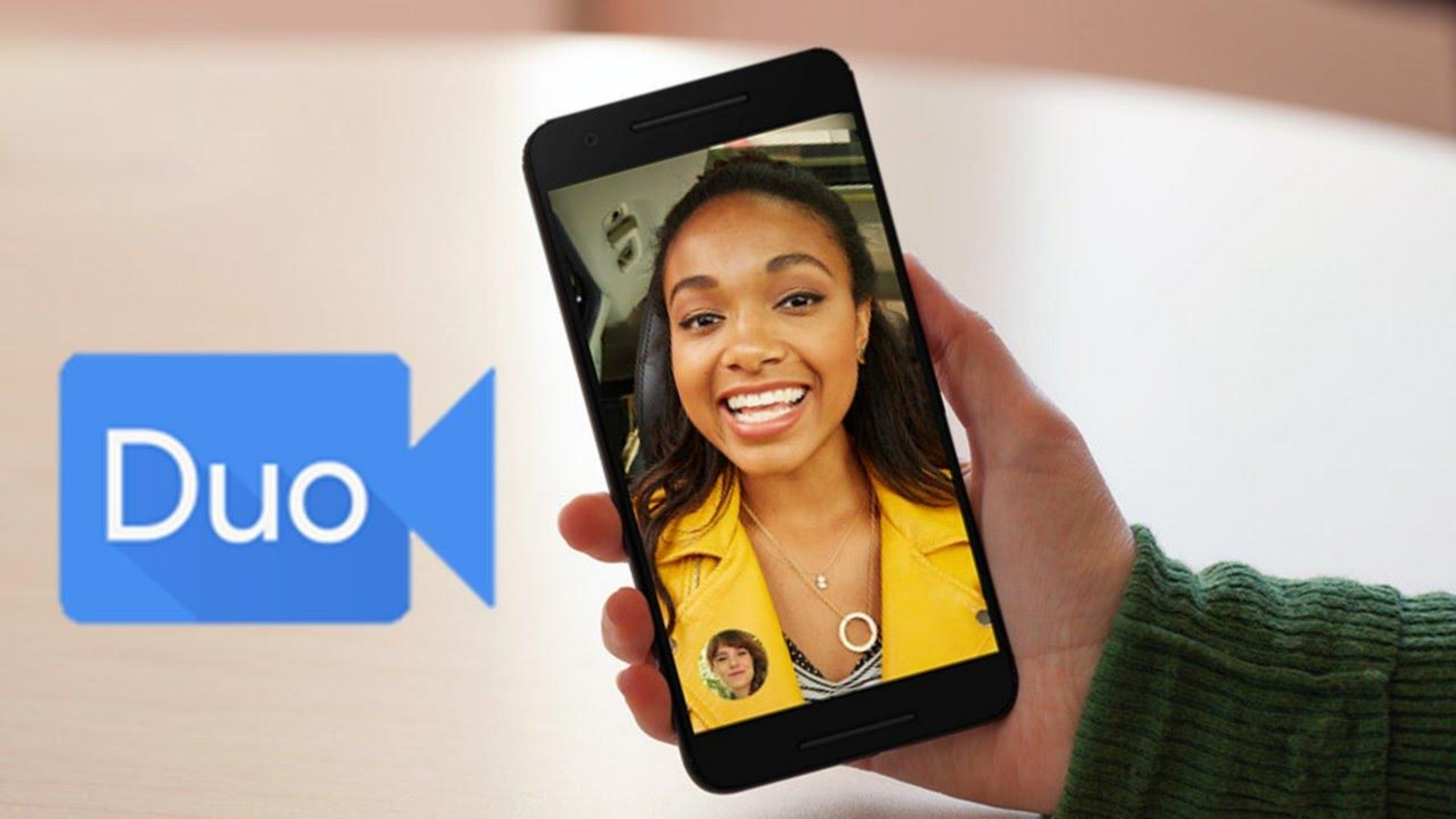


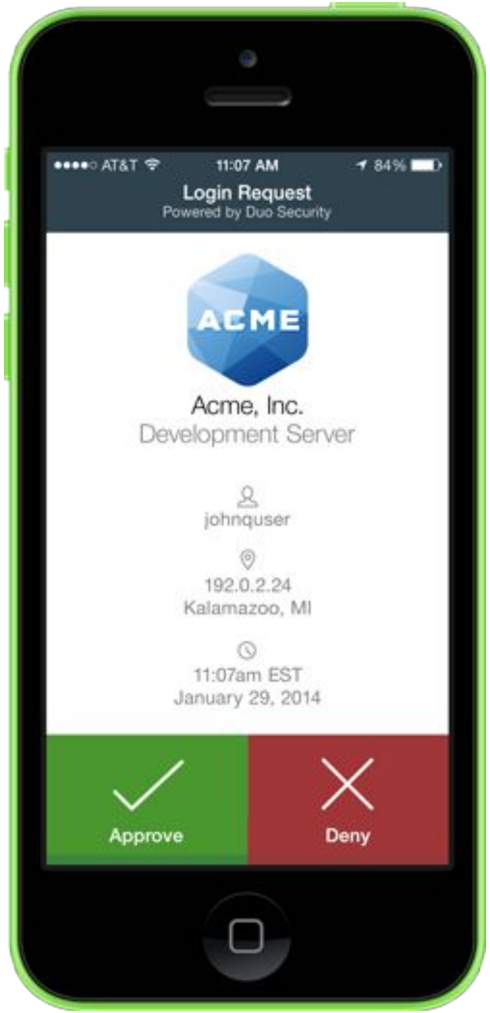
● Duo Labs / Feb 25, 2013

Bypassing Google's Two-Factor Authentication



RESEARCHERS FIND METHODS FOR BYPASSING GOOGLE'S BOUNCER ANDROID SECURITY


Duo



Login Request

Powered by Duo Security

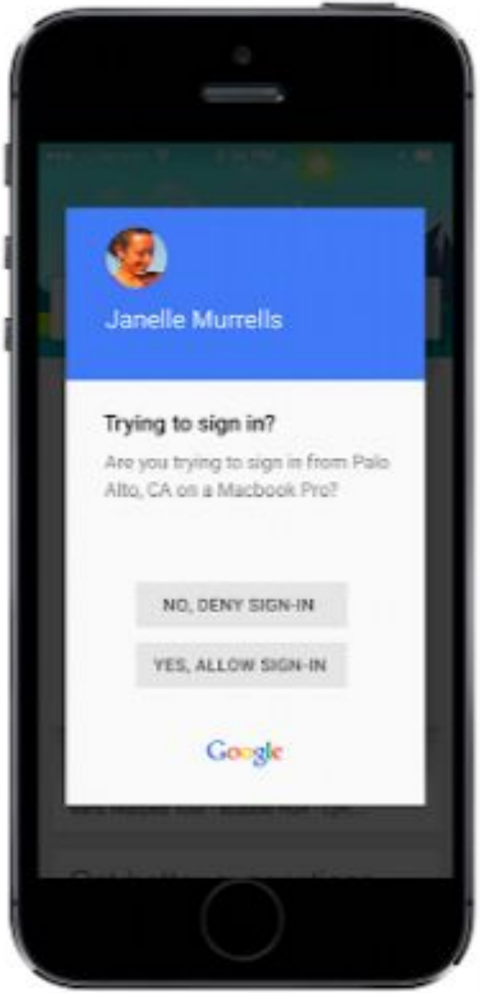
Acme, Inc.

Development Server

johnquser

192.0.2.24
Kalamazoo, MI

11:07am EST
January 29, 2014


Janelle Murrells

Trying to sign in?

Are you trying to sign in from Palo Alto, CA on a Macbook Pro?

Vision: Access

No "Perimeter"

Authentication

Authorization

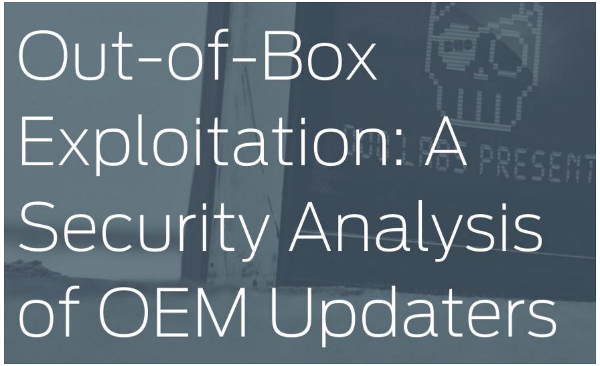
Encryption

The 2016 Duo Trusted Access Report

The Current State of Device Security

Android Security 2015 Year In Review

April 2016



Out-of-Box Exploitation: A Security Analysis of OEM Updaters

Project Zero

News and updates from the Project Zero team at Google

Tuesday, June 28, 2016

How to Compromise the Enterprise Endpoint

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

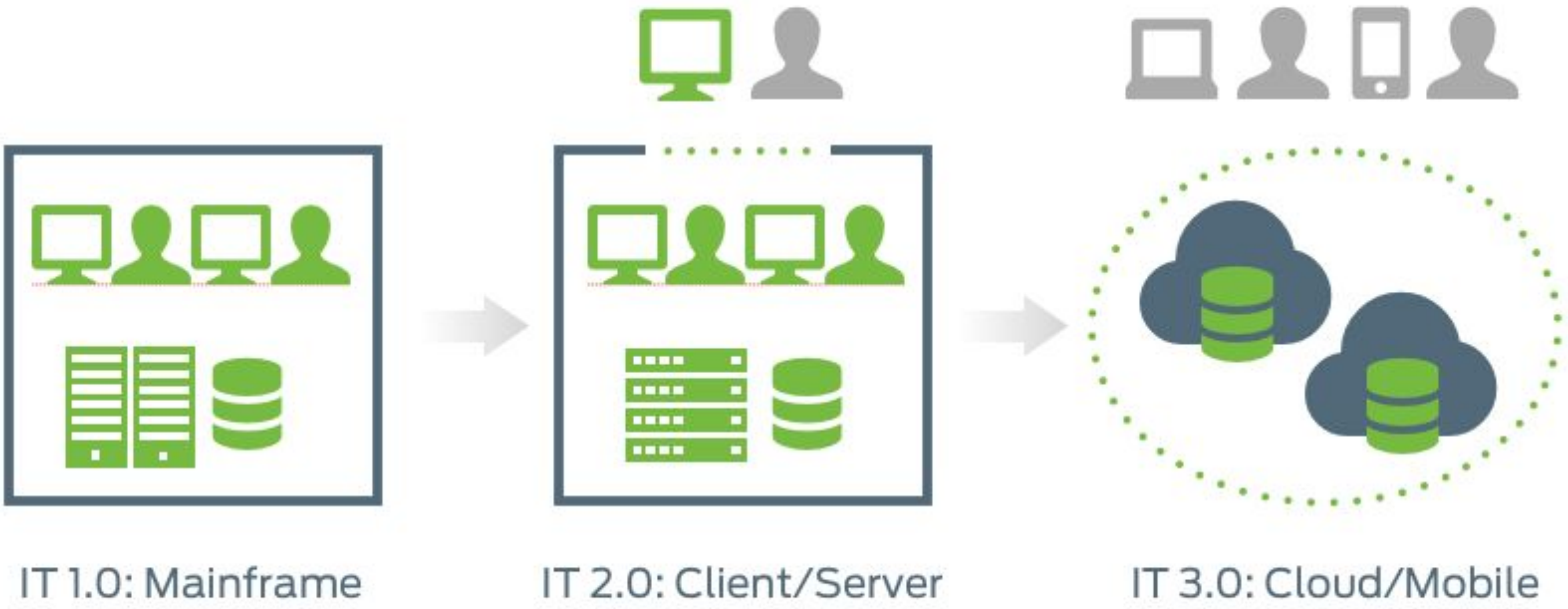
- Past
  - Gnubby / U2F
  - ATAP Trust Anchor
  - Beyond Corp / nassh
- Active
  - Android SafetyNet / Verified Boot
  - CrOS Verified Access
  - Sesame API
  - Project “Keep bothering Juan to get the gnubby ssh-agent applet”

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

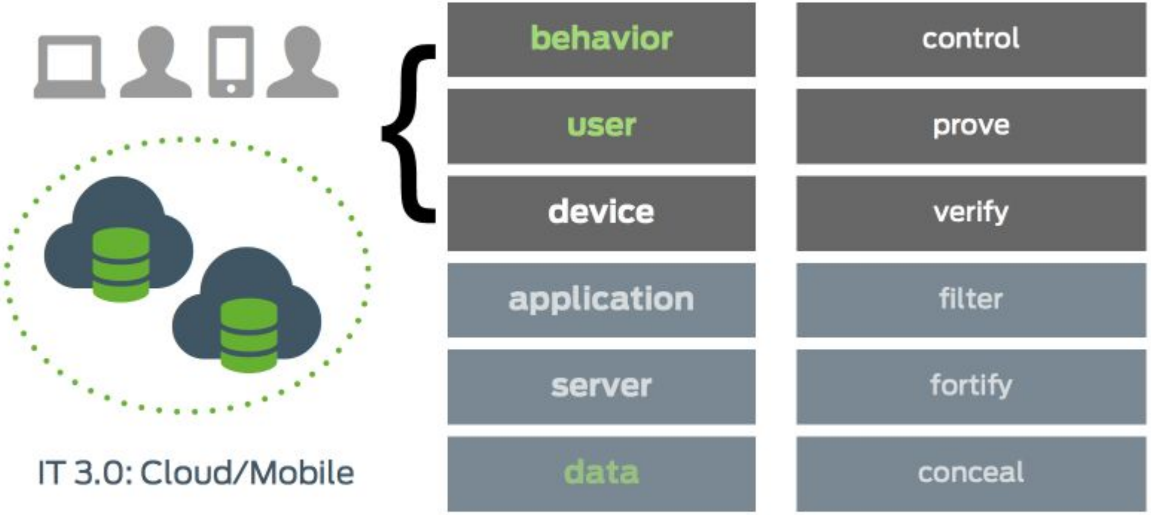
Where are we today?

Buzzword bingo: de-perimeterization!



Loss of traditional security controls

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



IT 3.0: Cloud/Mobile

behavior	control
user	prove
device	verify
application	filter
server	fortify
data	conceal

Targeting end users

95%

of breaches involve compromised **credentials**

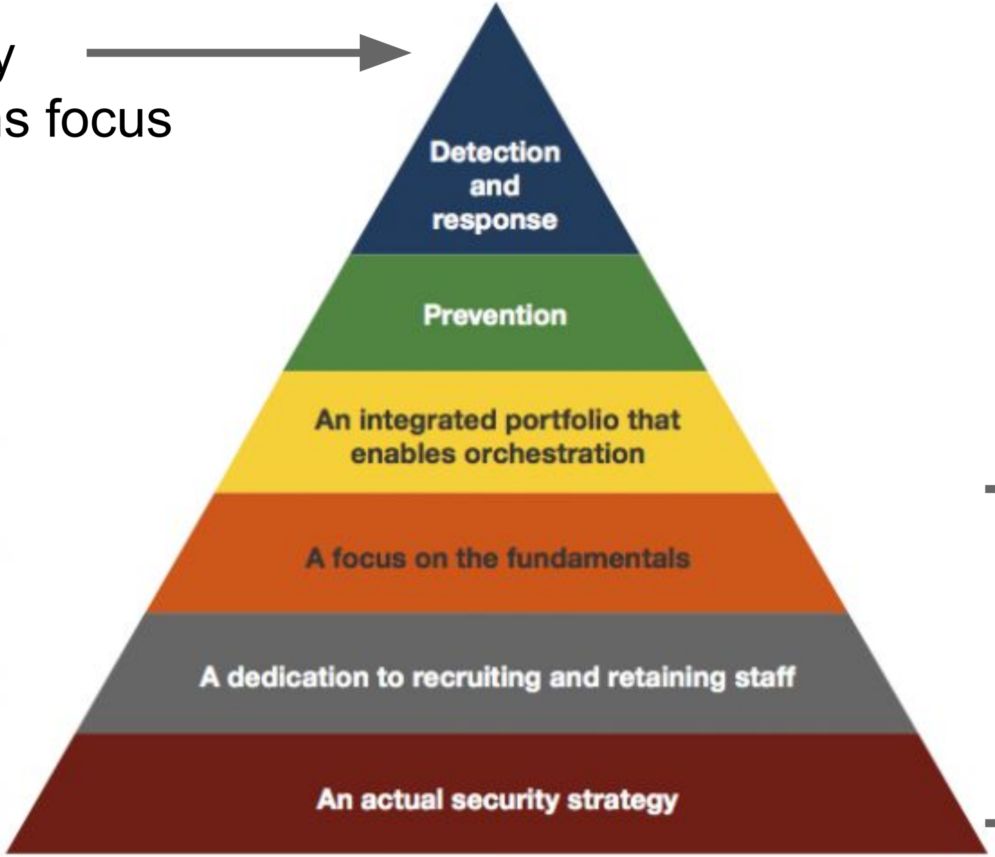
75%

of breaches involve compromised **devices**

Attackers are hijacking user access.

Focusing on the fundamentals

Where many organizations focus



Detection and response

Prevention

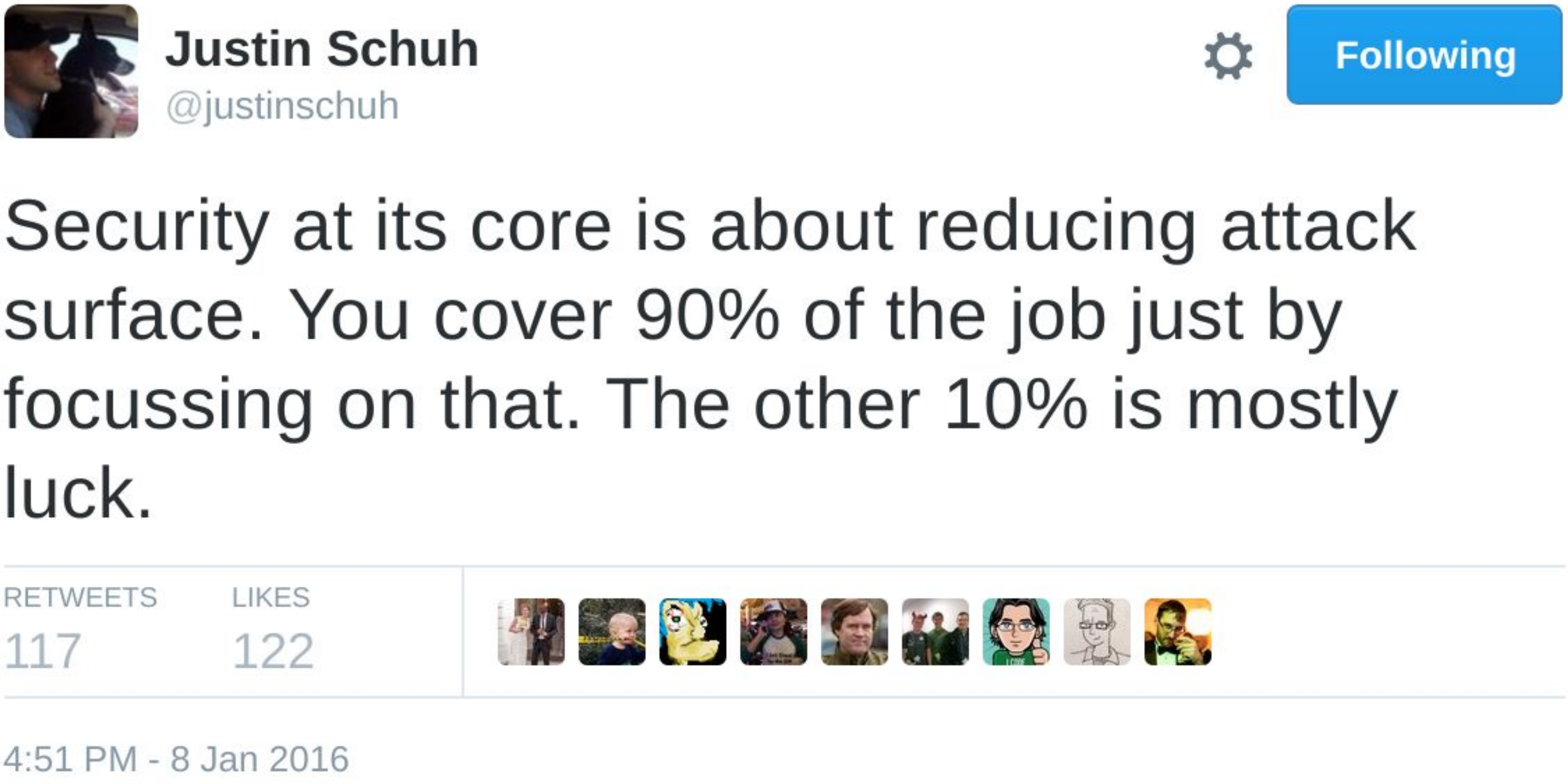
An integrated portfolio that enables orchestration

A focus on the fundamentals

A dedication to recruiting and retaining staff

An actual security strategy

Where we should focus



Justin Schuh
@justinschuh

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.

RETWEETS 117
LIKES 122

4:51 PM - 8 Jan 2016

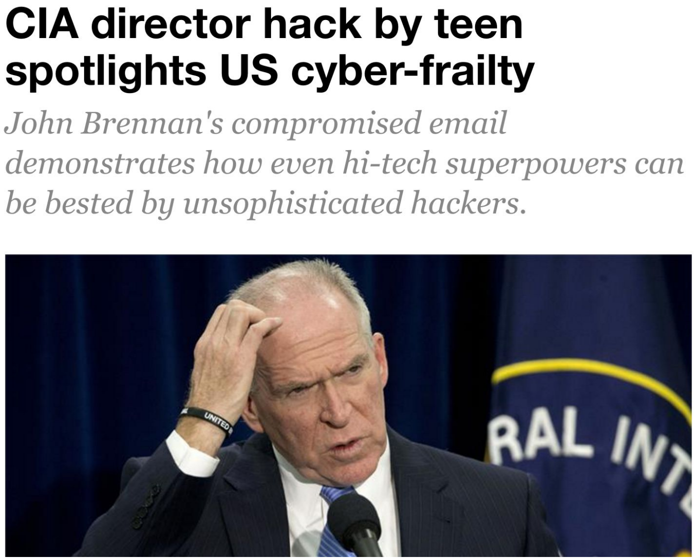
Eric Schmidt’s advice to Obama

✓ Strong Authentication

✓ Up-to-Date Devices

✓ Encryption

Haven’t quite nailed those...

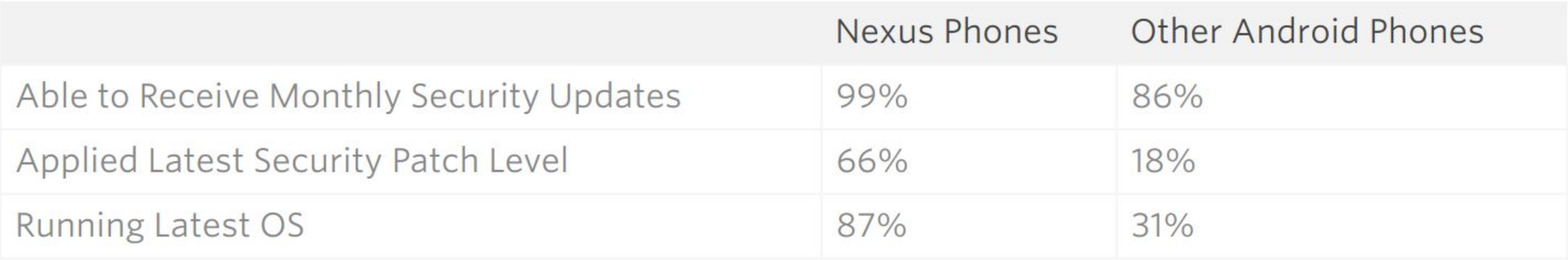


CIA director hack by teen spotlights US cyber-frailty

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

Lacking strong user auth

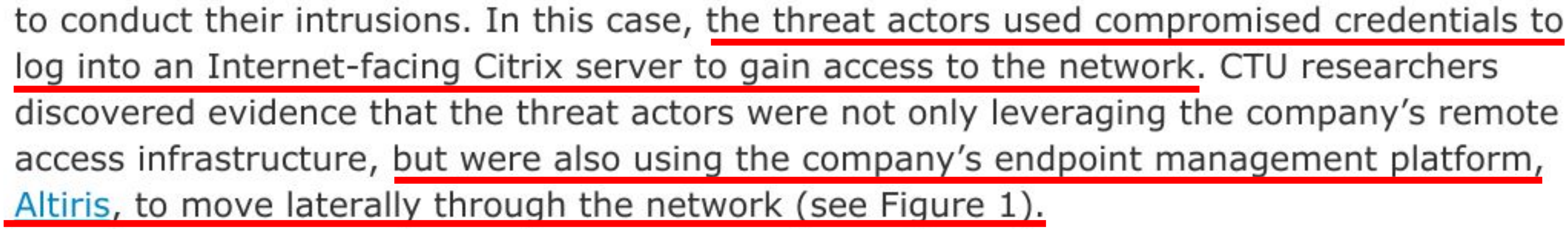
Pictured: Flash and Java



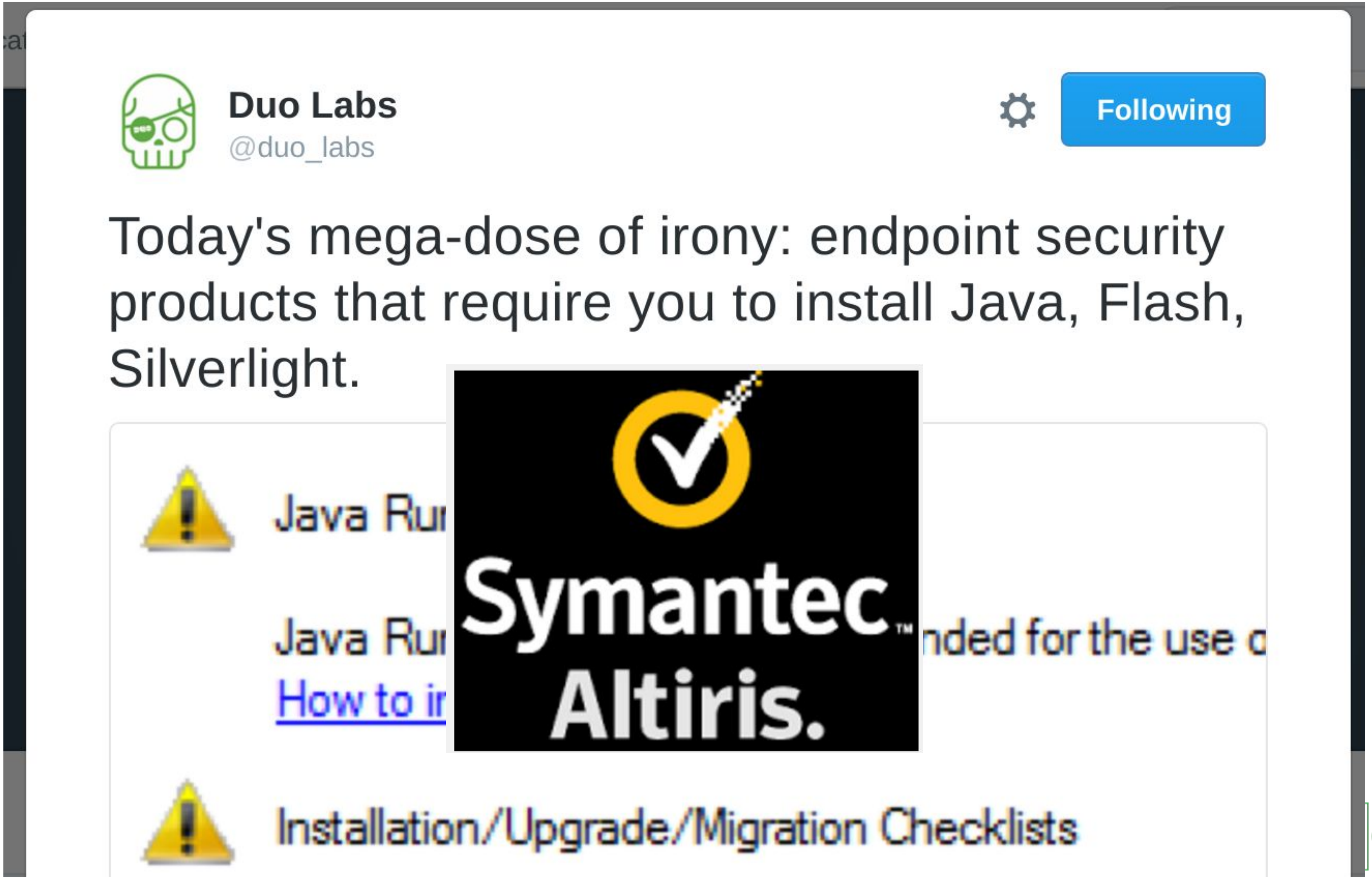
	Nexus Phones	Other Android Phones
Able to Receive Monthly Security Updates	99%	86%
Applied Latest Security Patch Level	66%	18%
Running Latest OS	87%	31%

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).



Duo Labs
@duo_labs

Today's mega-dose of irony: endpoint security products that require you to install Java, Flash, Silverlight.

Java Rur

Java Rur nded for the use c
How to ir

Installation/Upgrade/Migration Checklists

Release the Tavis!

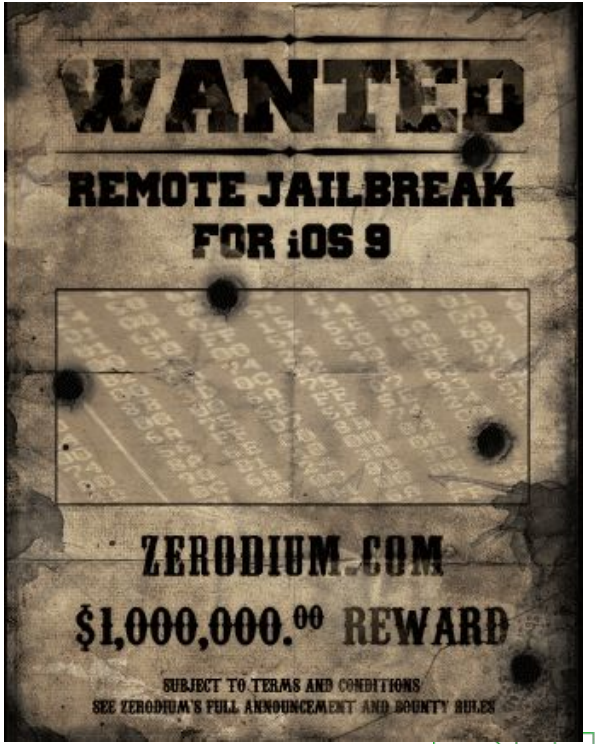
How do we get to a better place?

Progress in the face of breaches

Anthem
SONY
THE HOME DEPOT
TARGET

vs

.


WANTED
REMOTE JAILBREAK
FOR iOS 9
ZERODIUM.COM
$1,000,000.00 REWARD
SUBJECT TO TERMS AND CONDITIONS
SEE ZERODIUM'S FULL ANNOUNCEMENT AND BOUNTY RULES

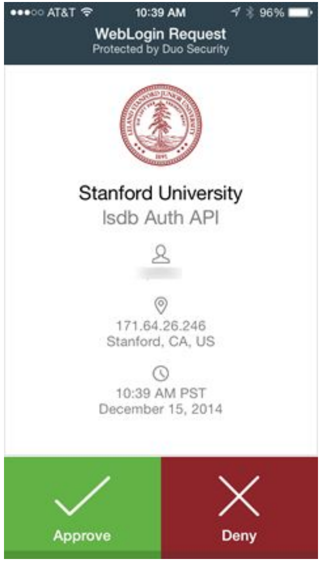
Who’s making it better?

vs

Google
Microsoft

User authentication

PAST


●●●○○ AT&T 10:39 AM 96%

WebLogin Request
Protected by Duo Security

Stanford University
lsdb Auth API

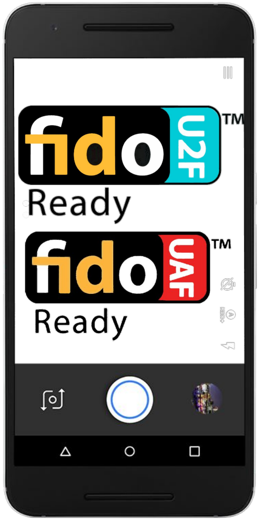
[redacted]

171.64.26.246
Stanford, CA, US

10:39 AM PST
December 15, 2014

**PRESEN
T**

**FUTUR
E**

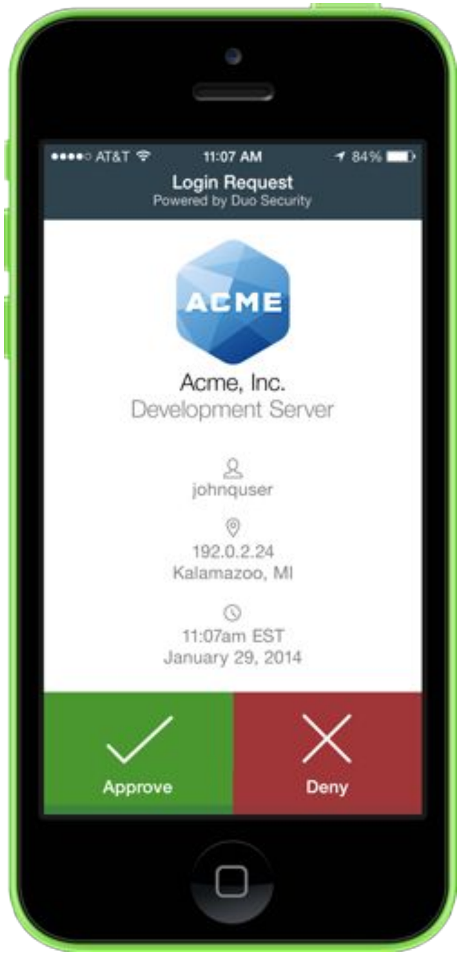


User authentication

- 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



●●●●○ AT&T 11:07 AM 84%

Login Request

Powered by Duo Security

Acme, Inc.

Development Server

johnquser

192.0.2.24

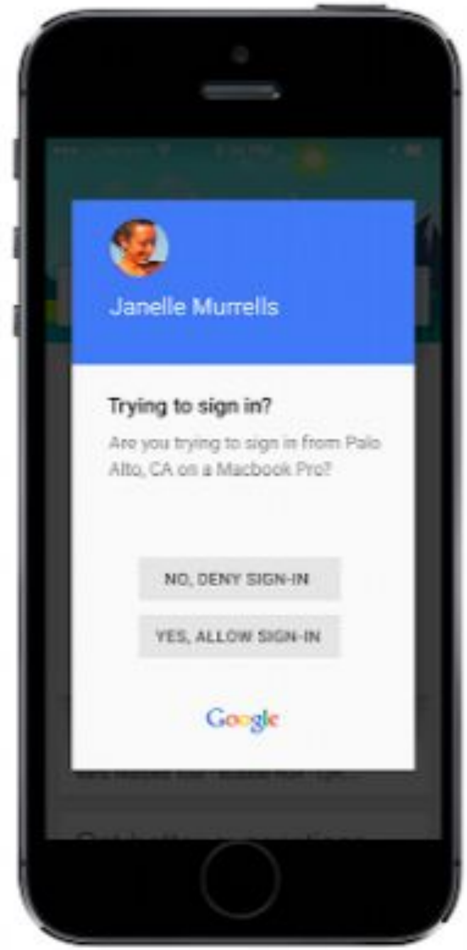
Kalamazoo, MI

11:07am EST

January 29, 2014

✓ Approve

✕ Deny



Janelle Murrells

Trying to sign in?

Are you trying to sign in from Palo Alto, CA on a Macbook Pro?

NO, DENY SIGN-IN

YES, ALLOW SIGN-IN

Google

U2F with YK4s

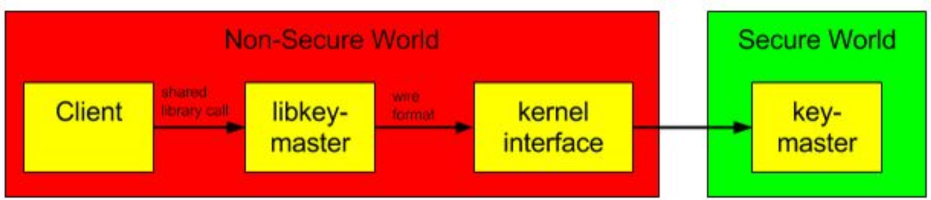
- “Unphishable”
- Easier than Push/Prompt
- Limited by hardware form factor, cost, deployment

Ideal state for user auth

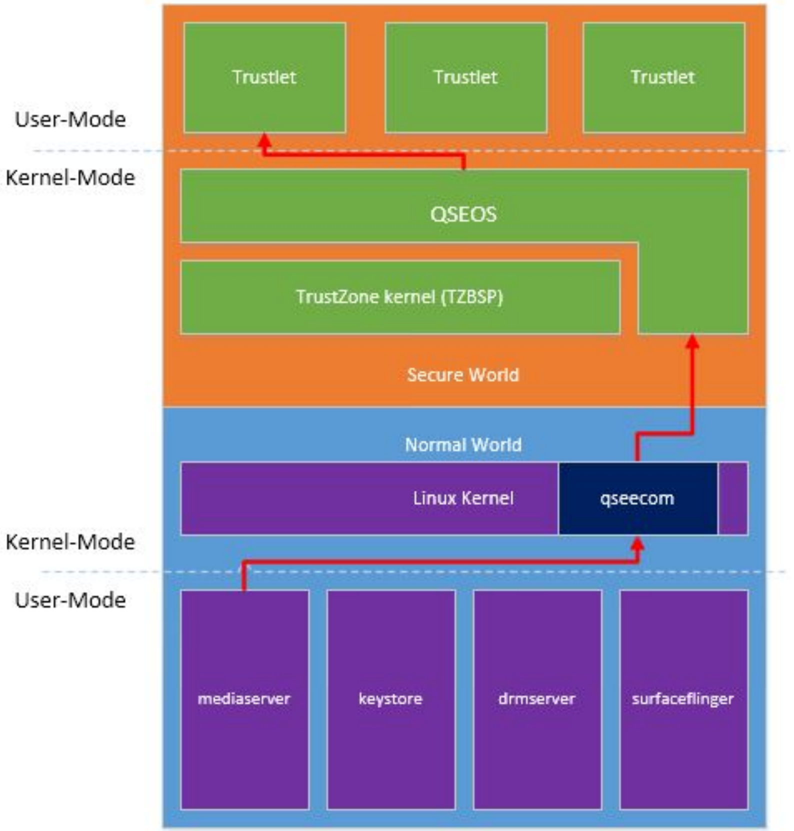
- Mobile device as root of trust
  - BTLE/NFC interfaces
- U2F/UAF credential in TEE
  - “Hardware-backed”
  - Built in to Android/iOS/Win10
- Unlock via biometric/KBA
  - Sesame for usability
  - Or TI/TD authz prompt

Hardware-backed security

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



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

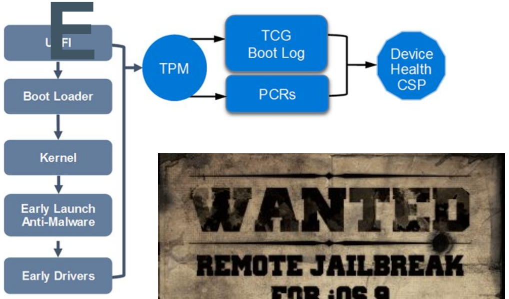


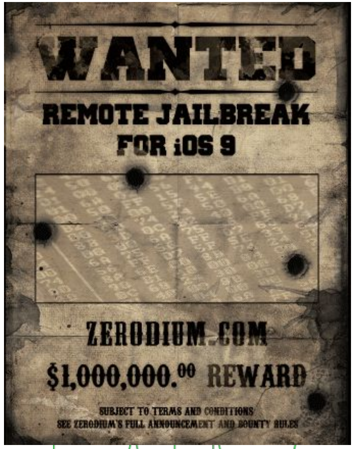
Device security

PAST

PRESENT

FUTUR
E





WANTED

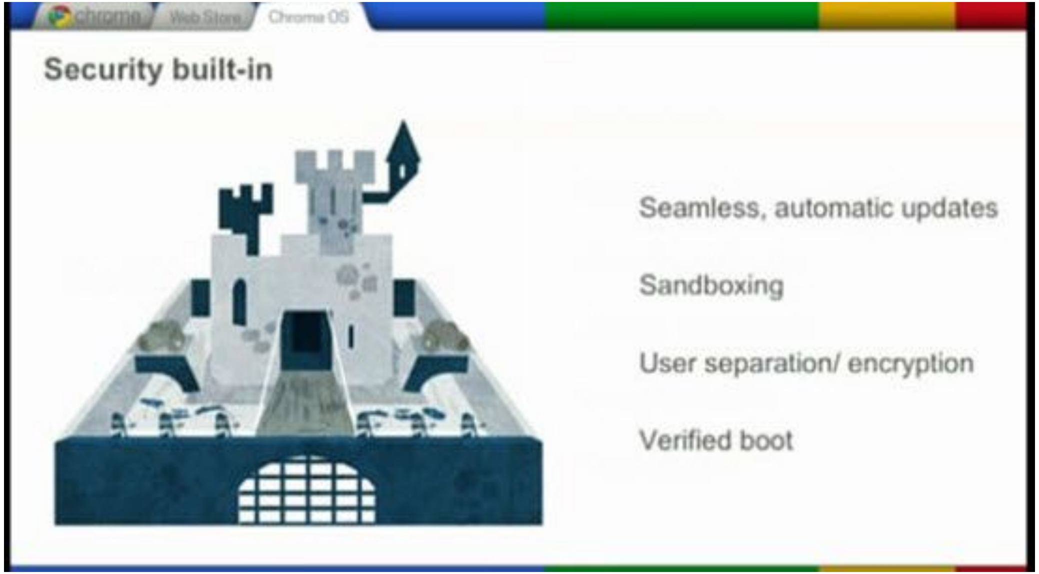
REMOTE JAILBREAK FOR iOS 9

ZERODIUM.COM

$1,000,000.00 REWARD

SUBJECT TO TERMS AND CONDITIONS
SEE ZERODIUM'S FULL ANNOUNCEMENT AND BOUNTY RULES

CrOS



Security built-in

Seamless, automatic updates

Sandboxing

User separation/ encryption

Verified boot

Remote health attestation

Windows 10

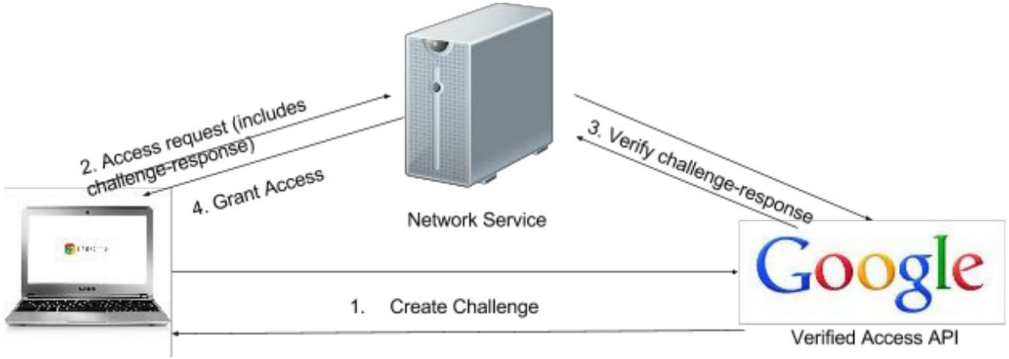
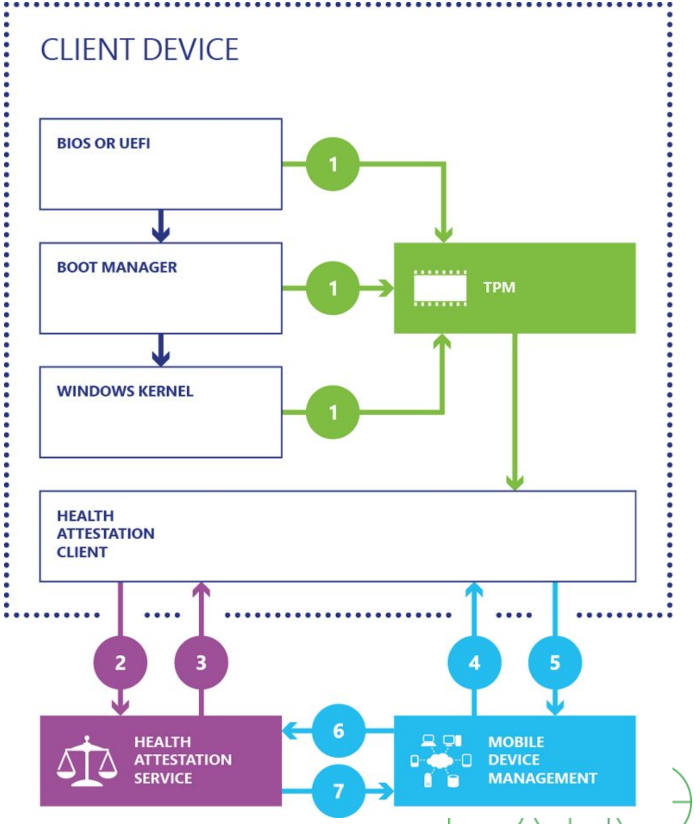

2. Access request (includes challenge-response)
4. Grant Access
Network Service
3. Verify challenge-response
Google
Verified Access API
1. Create Challenge

Figure 1. Suggested implementation

CrOS Verified Access

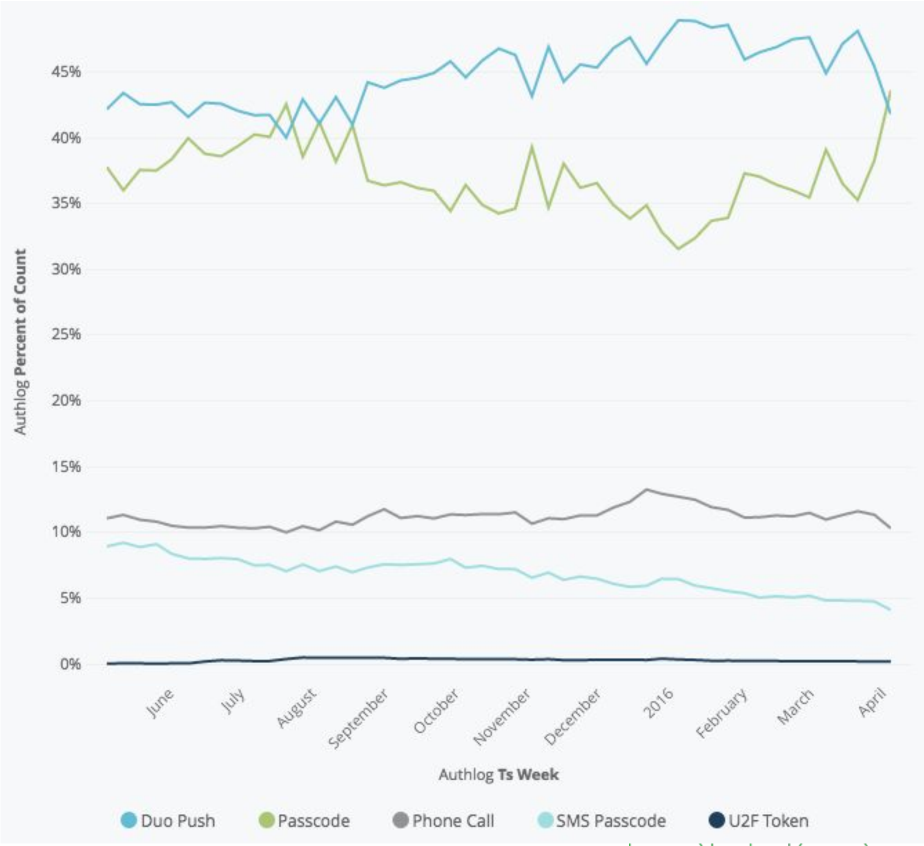


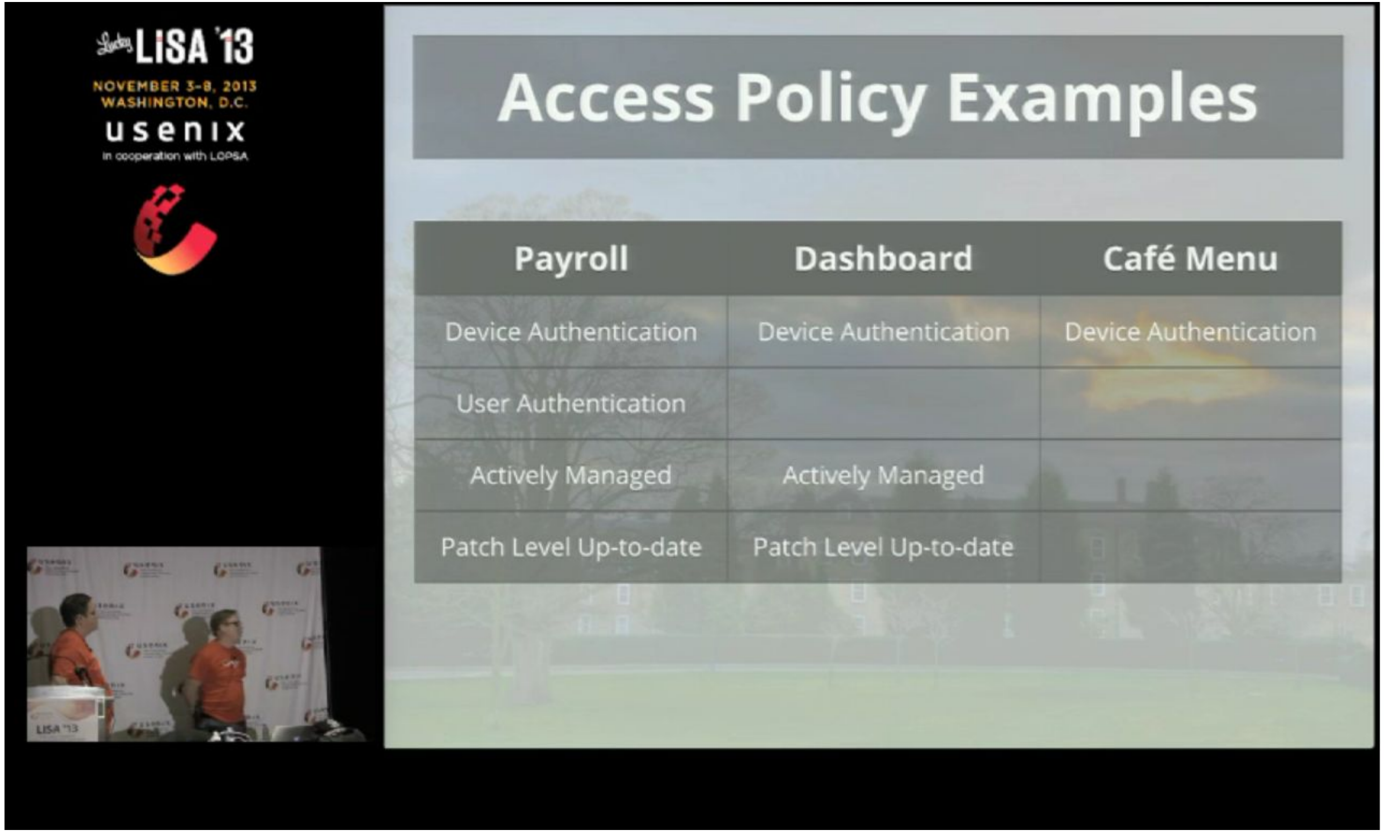
From bolt-on to built-in

“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





Access Policy Examples

Payroll	Dashboard	Café Menu
Device Authentication	Device Authentication	Device Authentication
User Authentication		
Actively Managed	Actively Managed	
Patch Level Up-to-date	Patch Level Up-to-date	

Tying these primitives into secure access and policy

Hard open problems

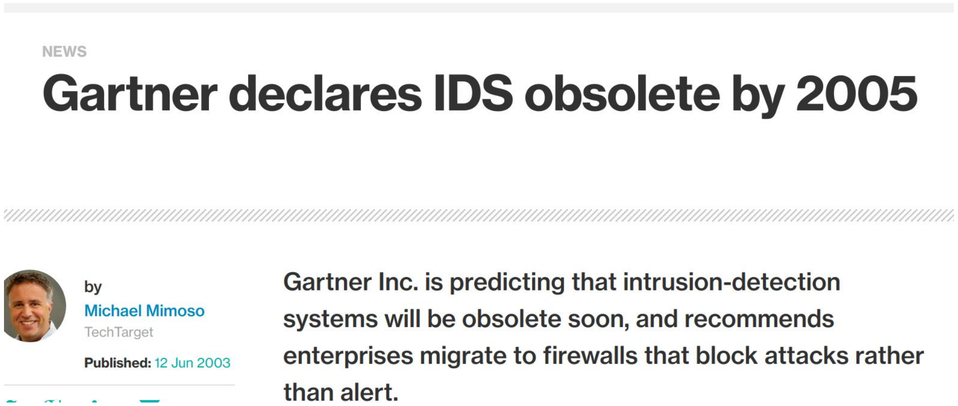
- Account recovery, credential bootstrapping
  - Ha!
- OAuth authz, scoping, phishing
  - Even easier than credential phishing
  - Pokemon Go, yay!
- Deep platform security
  - Firmware, AMT/ME, Ring -42
  - Joanna’s hypothetical stateless laptop

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



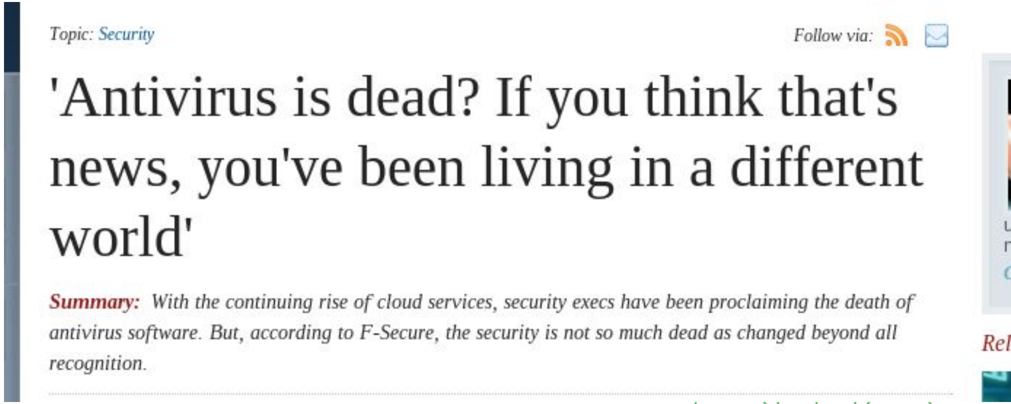
NEWS

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.



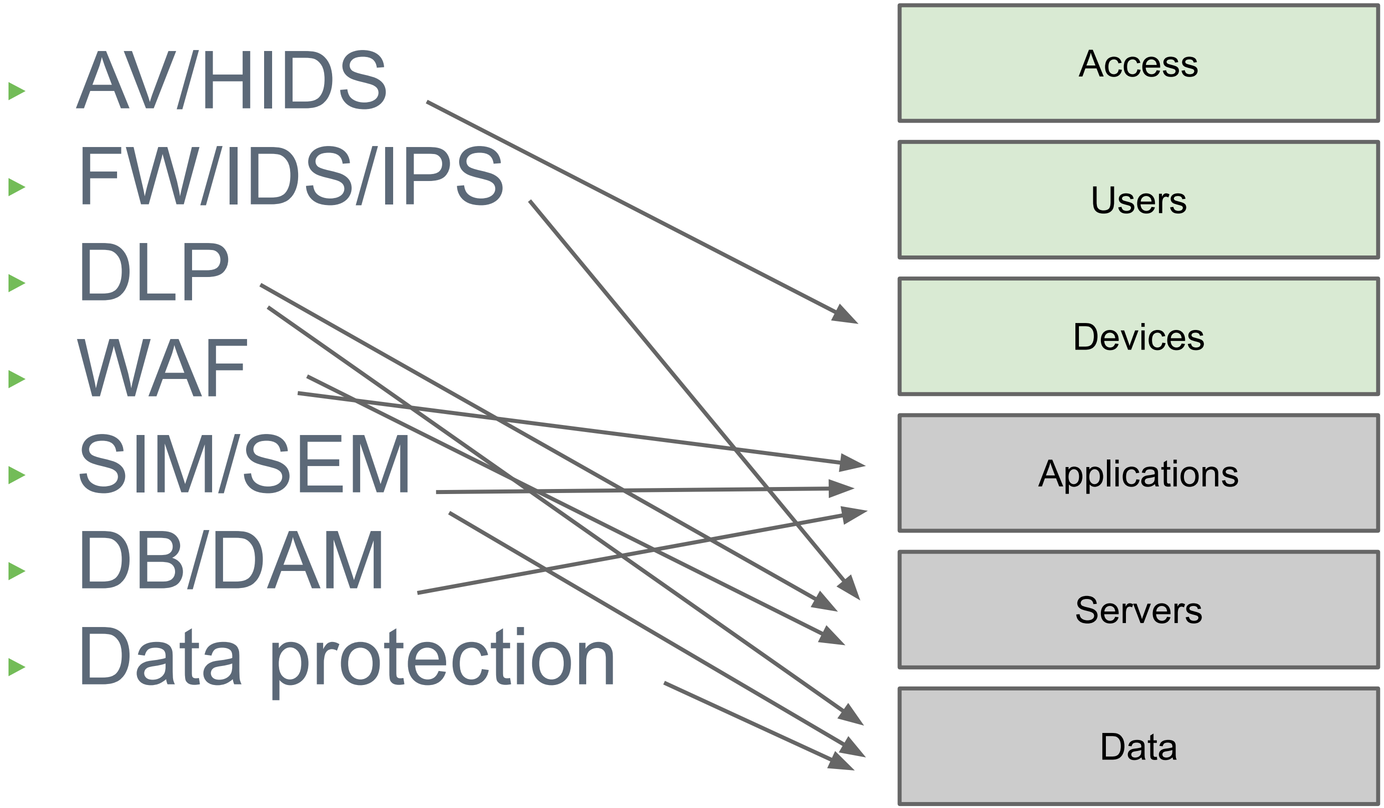
Topic: Security

Follow via:

'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

		Barracuda	CA	Check Point	Cisco	Dell	hp	IBM	McAfee intel	RSA EMC²	SafeNet	SOPHOS	Symantec	Trend Micro	Trustwave
Network Security	Firewall / VPN	■		■	■	■	■		■			■			■
	Unified Threat Management			■	■	■		■	■			■		■	■
	Intrusion Detection / Prevention			■	■		■	■	■	■					■
Web Security / Fraud Protection		■	■	■	■		■	■	■	■	■	■	■	■	■
Endpoint Security				■	■	■		■	■			■	■	■	
Mobile Security			■	■		■		■	■		■	■	■	■	■
Messaging / Encryption		■		■	■	■	■	■	■		■	■	■	■	■
Data Protection			■	■		■			■	■	■	■	■	■	■
Security and Vulnerability Management	Security Management		■		■	■	■	■	■	■			■	■	■
	Vulnerability Assessment						■	■	■	■			■		■
Identity and Access Management			■			■		■		■	■				

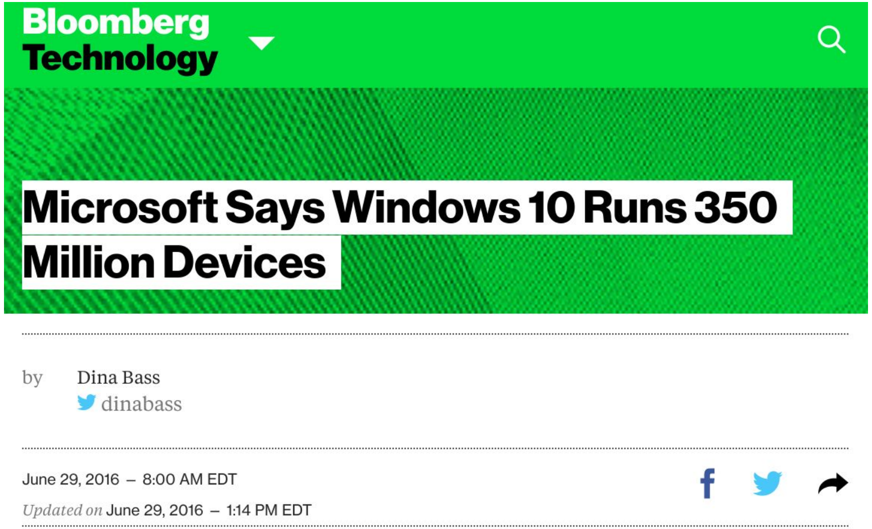
How far is the “future”?

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

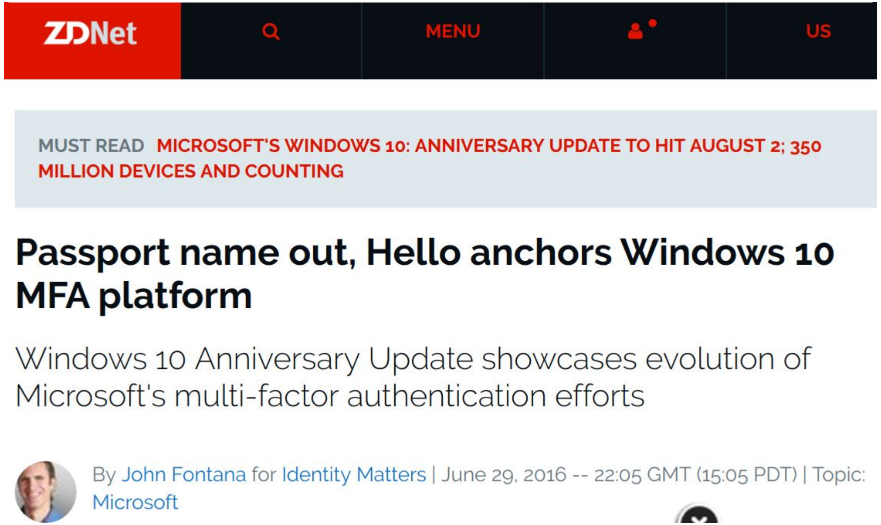


Bloomberg Technology

Microsoft Says Windows 10 Runs 350 Million Devices

by Dina Bass
dinabass

June 29, 2016 – 8:00 AM EDT
Updated on June 29, 2016 – 1:14 PM EDT

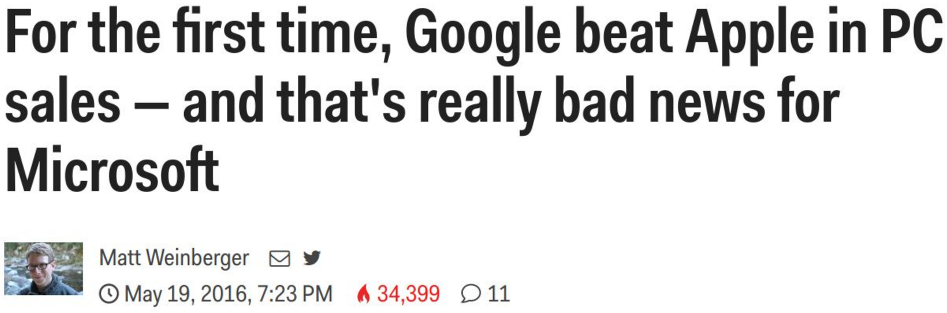


MUST READ MICROSOFT'S WINDOWS 10: ANNIVERSARY UPDATE TO HIT AUGUST 2; 350 MILLION DEVICES AND COUNTING

Passport name out, Hello anchors Windows 10 MFA platform

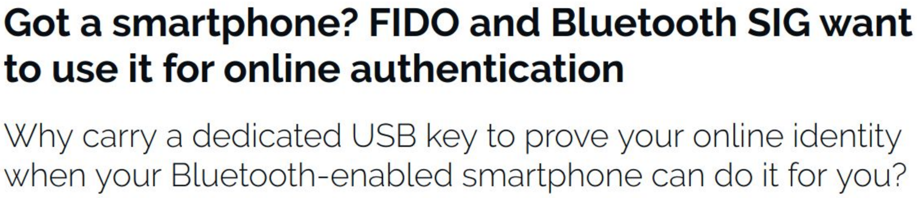
Windows 10 Anniversary Update showcases evolution of Microsoft's multi-factor authentication efforts

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



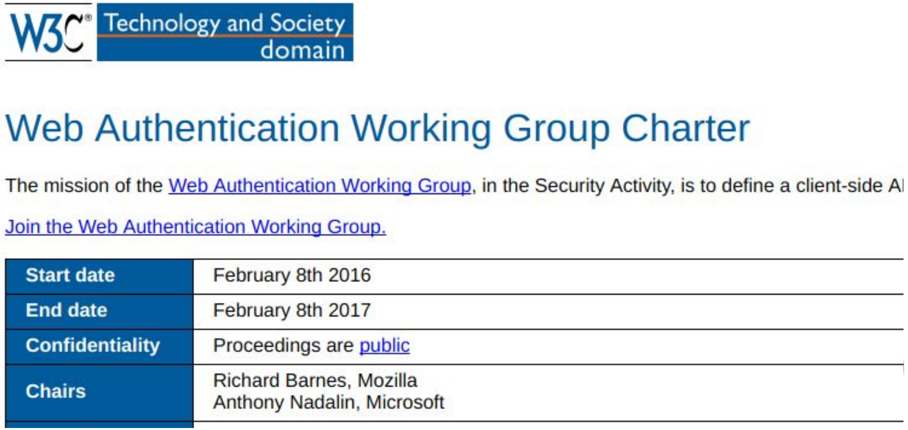
For the first time, Google beat Apple in PC sales — and that's really bad news for Microsoft

Matt Weinberger
May 19, 2016, 7:23 PM 34,399 11



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?



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.

Start date	February 8th 2016
End date	February 8th 2017
Confidentiality	Proceedings are public
Chairs	Richard Barnes, Mozilla Anthony Nadalin, Microsoft

Legacy long tail

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