Fundamentals, Fears, and Futures

Jon Oberheide

CTO, Duo Security

jono@duosecurity.com

Hacking the Planet

UNIVERSITY OF MICHIGAN

PhD Researcher

Co-Founder & CTO

NORTH AMERICAN INTERNATIONAL CYBER SUMMIT 2016

October 17

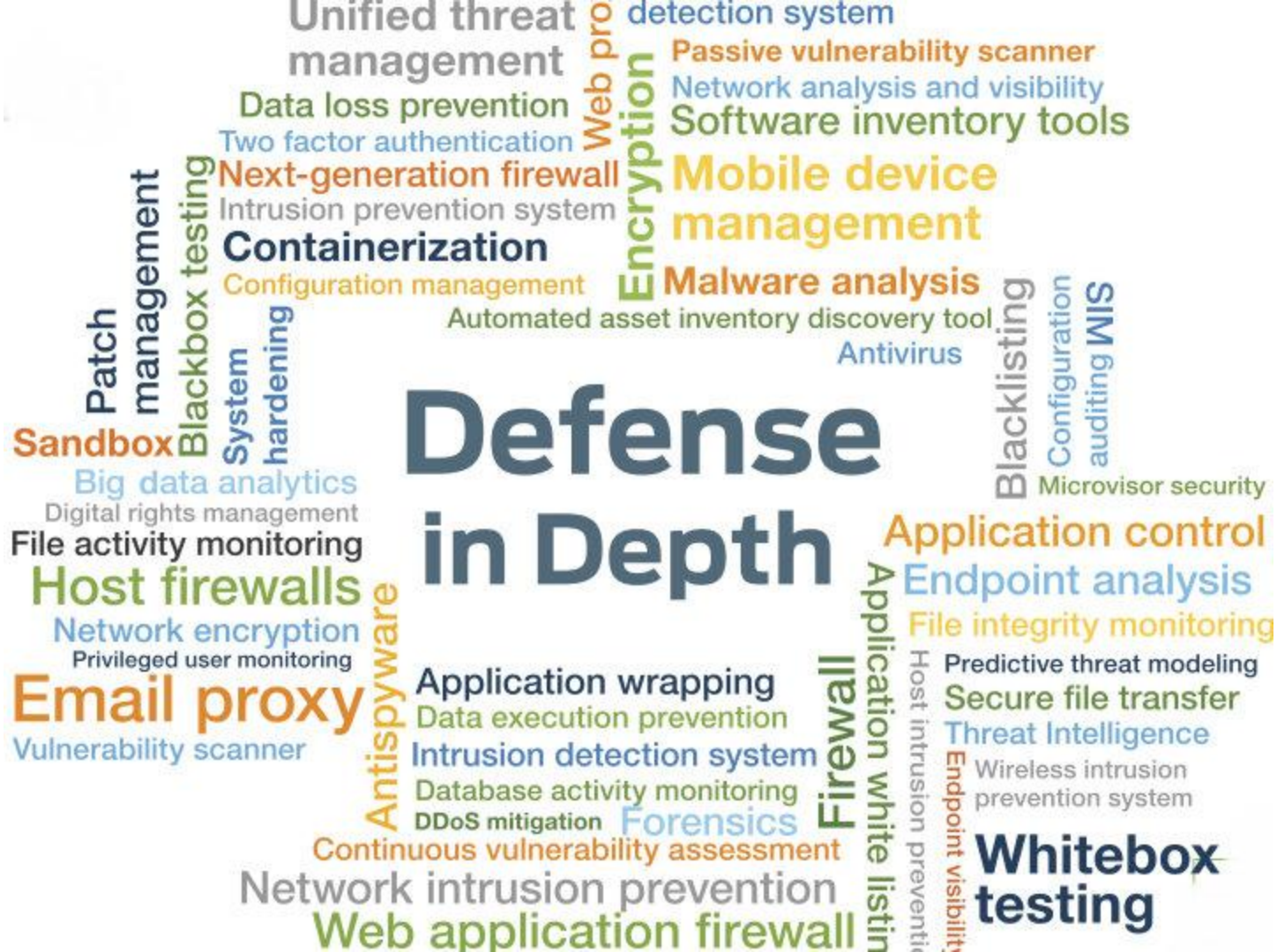
Talking to you!

Ok, let's make claims!

- ~30 minutes to make some claims
  - Industry dysfunction and FUD
  - Fundamentals of security
  - The future of security
- ~15 minutes to tell me how I'm wrong
  - Aka Q&A

Don’t buy security products.

...besides Duo. ;-)


Defense in Depth
Unified threat management
Data loss prevention
Two factor authentication
Next-generation firewall
Intrusion prevention system
Containerization
Configuration management
Web pro
detection system
Passive vulnerability scanner
Network analysis and visibility
Software inventory tools
Encryption
Mobile device management
Malware analysis
Automated asset inventory discovery tool
Antivirus
Patch management
Blackbox testing
System hardening
Sandbox
Big data analytics
Digital rights management
File activity monitoring
Host firewalls
Network encryption
Privileged user monitoring
Email proxy
Vulnerability scanner
Antispyware
Application wrapping
Data execution prevention
Intrusion detection system
Database activity monitoring
DDoS mitigation
Forensics
Continuous vulnerability assessment
Network intrusion prevention
Web application firewall
Firewall
Application white listing
Host intrusion prevention
Blacklisting
Configuration auditing
WIS
Microvisor security
Application control
Endpoint analysis
File integrity monitoring
Predictive threat modeling
Secure file transfer
Threat Intelligence
Endpoint visibility
Wireless intrusion prevention system
Whitebox testing


Unified threat management
Data loss prevention
Two factor authentication
Next-generation firewall
Intrusion prevention system
Containerization
Configuration management
Web pro
detection system
Passive vulnerability scanner
Network analysis and visibility
Software inventory tools
Encryption
Mobile device management
Malware analysis
Automated asset inventory discovery tool
Antivirus
Patch management
Blackbox testing
System hardening
Sandbox
Big data analytics
Digital rights management
File activity monitoring
Host firewalls
Network encryption
Privileged user monitoring
Email proxy
Vulnerability scanner
Expense in Depth
Blacklisting
Configuration auditing
WIS
Microvisor security
Application control
Endpoint analysis
File integrity monitoring
Predictive threat modeling
Secure file transfer
Threat Intelligence
Wireless intrusion prevention system
Application white listing
Host intrusion prevention
Endpoint visibility
Antispyware
Application wrapping
Data execution prevention
Intrusion detection system
Database activity monitoring
DDoS mitigation
Forensics
Continuous vulnerability assessment
Network intrusion prevention
Web application firewall
Firewall
Whitebox testing

Complexity breeds insecurity.

Reduce complexity and attack surface.

Justin Schuh
@justinschuh

Following

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

Duo Labs
@duo_labs

Following

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

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).

DELL SecureWorks

Don’t buy a new security product unless it allows you decommission two.

31

Like

Share

120

Tweet

120

Share

8

Adam Greenberg, Reporter

Follow @writingadam

March 13, 2014

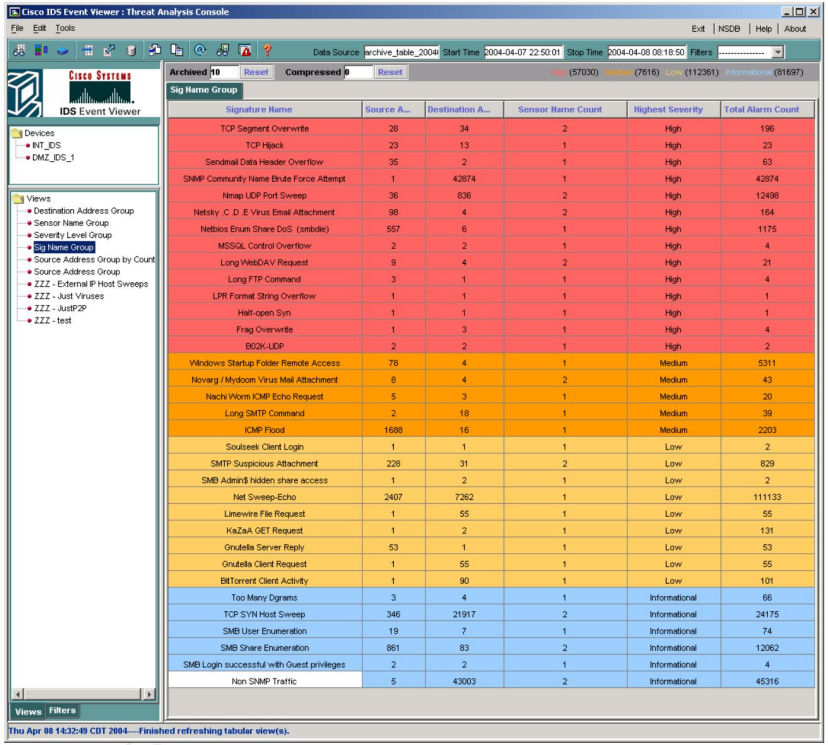
Target did not respond to FireEye security alerts prior to breach, according to report

Share this article:

Target might have been a tad negligent when it came to observing its security systems last year,

Don’t be a scope dope

- Avoid security tech that creates busy work for your team
- If it’s not actively making your live easier, trash it.



Customer observations

Our most sophisticated customers are:

- Only buying like 3 security products
- Favoring build over buy
- Hiring security engineers instead of admins
- Tailoring security solutions to their org/threats

Ignore APTs.


FireEye
Subscribe to FireEye Alerts
[X] NEW ATTACK: FROM
[X] NEW ATTACK: FROM
[X] NEW ATTACK: FROM
[X] NEW ATTACK: FROM
CYBE
UNITED STATES
ATTACKERS
TOP COUNTRIES
(PAST 30 DAYS)
TARGETS
TOP COUNTRIES
(PAST 30 DAYS)
The "Cyber Threat Map" is b


The Economist
Why fairness is a bad idea
Rewriting Wall Street's rules
Who will run Brazil?
How Big Oil became Big Gas
The link between IQ and disease
JULY 3RD–9TH 2010
Economist.com
Cyberwar
The threat from the internet
€5.50


VS.
SONY
PICTURES

Use Duo@duo.sc
Stop guessing at attribution
North
Korea

APT ≡ Average Phishing Technique

Targeting end users

95%

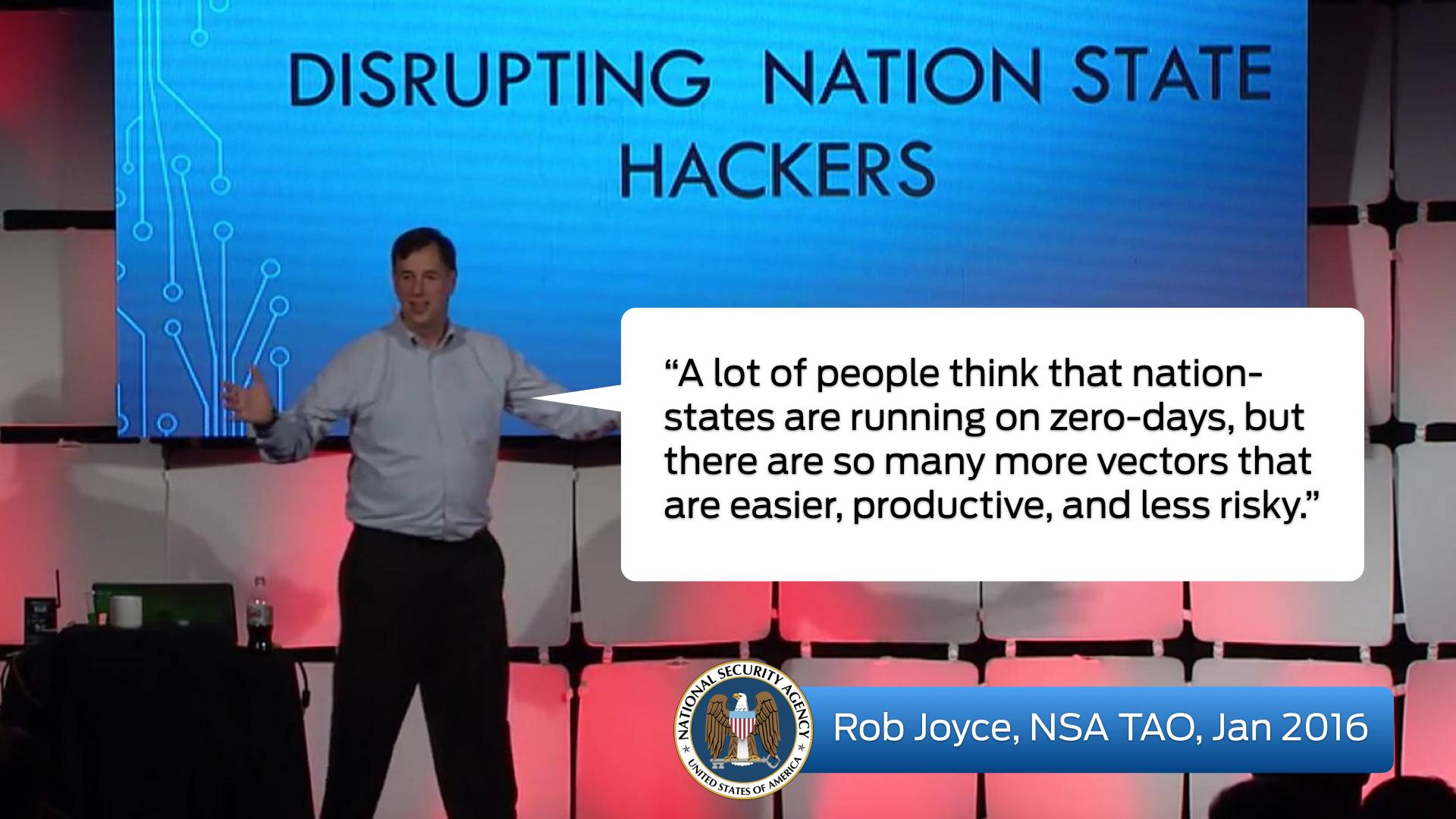
of breaches involve compromised **credentials**

75%

of breaches involve compromised **devices**

Attackers are targeting end users directly and *hijacking access* to apps/data


DISRUPTING NATION STATE HACKERS
“In the world of advanced persistent threat actors, credentials are king for gaining access to systems.”
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
Rob Joyce, NSA TAO, Jan 2016


DISRUPTING NATION STATE HACKERS
“A lot of people think that nation-states are running on zero-days, but there are so many more vectors that are easier, productive, and less risky.”
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
Rob Joyce, NSA TAO, Jan 2016

Focus on the fundamentals.

Focusing on the fundamentals

Where many organizations focus

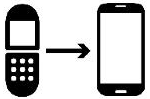
Where we should focus

Eric Schmidt's advice to Obama

- ✓ Strong Authentication
- ✓ Up-to-Date Devices
- ✓ Encryption

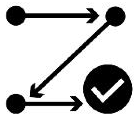
President Obama's $19 Billion Cybersecurity Proposal Calls for 35% Increase Over 2016 Enacted Level

Major Pieces of the Cybersecurity National Action Plan



$3.1 billion Information Technology Modernization Fund
This fund enables the retirement, replacement and modernization of IT equipment throughout the government. Many see this initiative as overdue as some branches of the government are running antiquated as old as Windows XP which Microsoft stopped officially supporting in 2014.

← Up to date devices



Full Multi-Step Authentication Rollout
While a large portion of the government uses 2-step or multi-step authentication for internal logins, the initiative plans to extend this extra layer of security to citizen-facing federal government digital services. The President hopes this switch will also increase public awareness of this identity proofing mechanism, encouraging more wide use among private online systems.

← Strong authentication

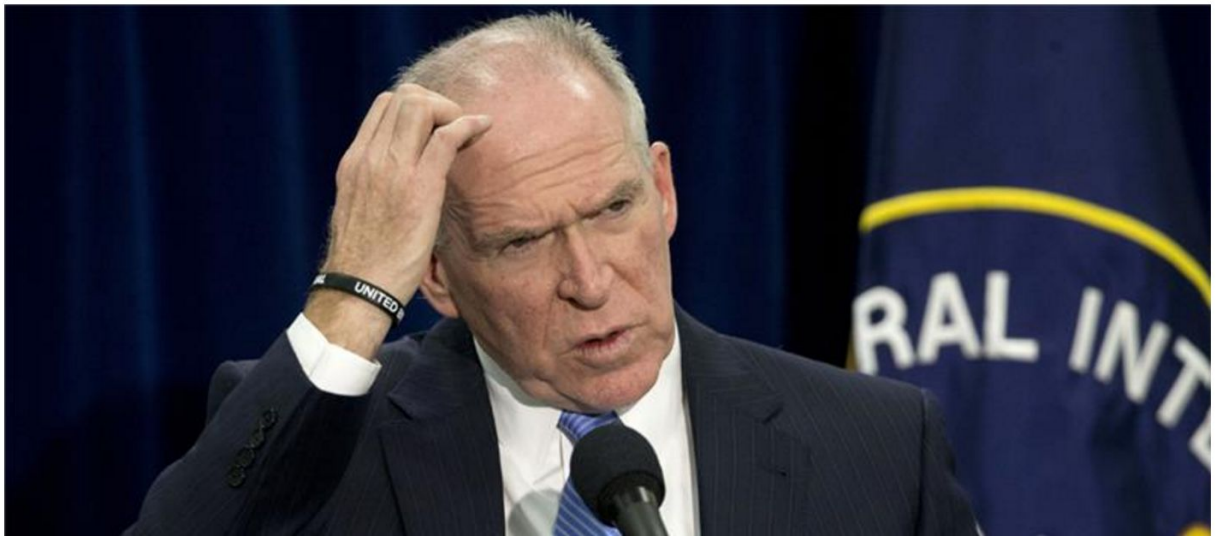
EINSTEIN and the Continuous Diagnostic and Mitigation Program
The president proposes allocating increased funding to the government's primary cyberdefense system: EINSTEIN, which has faced significant criticism since it is currently unable to dynamically detect new kinds of cyber intrusions, making it only useful against known threats.

No encryption?!? THANKS OBAMA. :-(

National Initiative for Cybersecurity Education
$62 billion is requested to invest in educating the nation's next generation of cybersecurity personnel. Proposed programs include the CyberCorps Reserve which would offer scholarships for Americans who wish to obtain cybersecurity education in exchange for civil service in government.

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.



Data at Duo

Mobile: Android and iOS

71%

of Android devices out of date

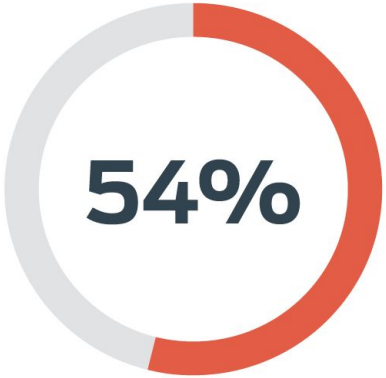
Android < 5.1.1 or < 6.0.1

50%

of iOS devices out of date

iOS < 9.2

Operating systems: OS X



of Macs either run an **unsupported OS**, or are **not fully patched**.

of all Macs are **not running the latest major version**, 10.11.

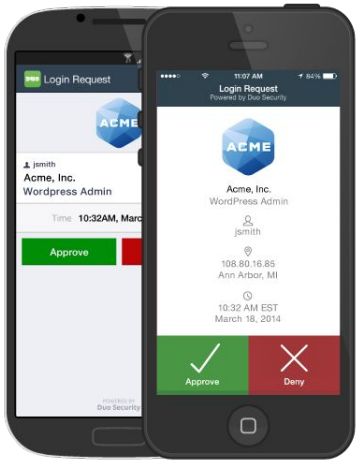
Web browsers: Firefox

- New version of Firefox released in Dec 2015.
- After 23 days, only **50%** of browsers had updated.
- Peaked at **69%** at 42 days, then a new version of Firefox came out.

Plugins: Flash and Java

Basic security hygiene

What we should be doing:

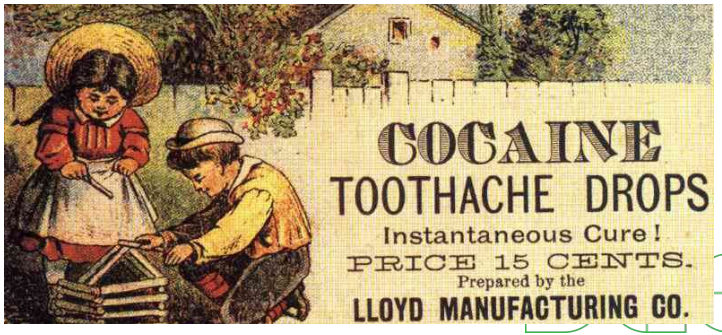


What we're doing instead:

Basic security hygiene

What we should be doing:

What we're doing instead:



Do uncomfortable things.

Do this to your current security program.

Turn your corporate network inside out.

Buzzword bingo: de-perimeterization!

LISA '13
NOVEMBER 3-8, 2013
WASHINGTON, D.C.
usenix
in cooperation with LOPSA

Google

Vision: Access

No "Perimeter"

Authentication

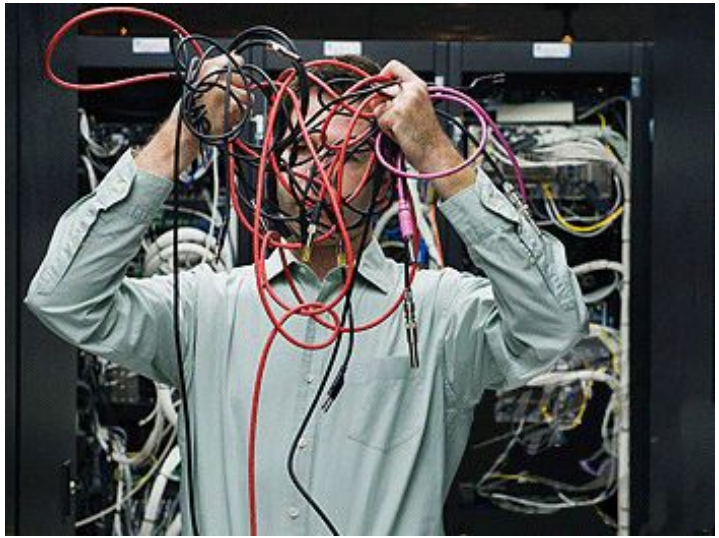
Authorization

Encryption


LISA '13
NOVEMBER 3–8, 2013
WASHINGTON, D.C.
usenix
in cooperation with LOPSA
Google
Vision: User Experience
work from anywhere
cloud based workflows
limit access by policy only
07:19

Go all-in cloud.

Security operations



vs

.

Google

Microsoft

amazon web services

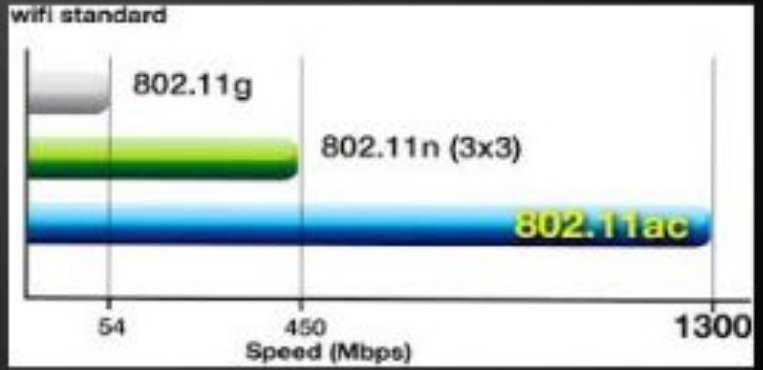
10X Goal for 2014

100% of Corporate IT in SaaS/Public Cloud

"SOUNDS GREAT, BUT HOW DO WE ACCOMPLISH THIS?"

Identity Is The New Perimeter

- Zero Trust Network Architecture
  - Core Network Stability is priority #1
  - Aruba 802.11ac upgrade
  - VPN required to DC from everywhere
  - Certificate-Based Auth to Nightmares
    - EJBCA
    - Aruba ClearPass



Trust your users.


MORDAC, THE PREVENTER OF INFORMATION SERVICES.
SECURITY IS MORE IMPORTANT THAN USABILITY.
www.dilbert.com
scottadams@aol.com
IN A PERFECT WORLD, NO ONE WOULD BE ABLE TO USE ANYTHING.
11-16-07
©2007 Scott Adams, Inc./Dist. by UFS, Inc.
To complete the log-in procedure, stare directly at the sun.

Ryan Huber

Feb 29 · 5 min read

Distributed Security Alerting

securitybot BOT 12:47 PM

I see you just ran the command `flurb -export` on `accountingserver01`. This is a sensitive command, so please acknowledge this activity by typing `acknowledge`.

ryan 12:47 PM

acknowledge

securitybot BOT 12:47 PM

Acknowledging via 2fa.

What would you change tomorrow if you were breached?

Do that today.

Security is getting better.

Seriously.

Uh, do you read the news?

Anthem

SONY

THE HOME DEPOT

TARGET

vs

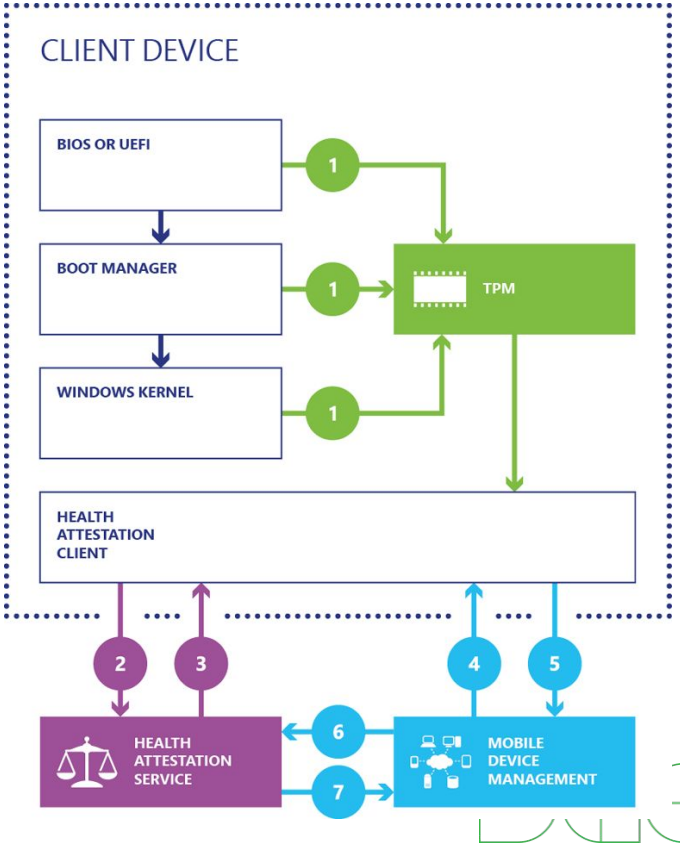
.

Ex: Chrome, CrOS

Ex: Hardware-backed unphishable auth

Ex: Remote health attestation

Windows 10



Who’s making it better?

vs

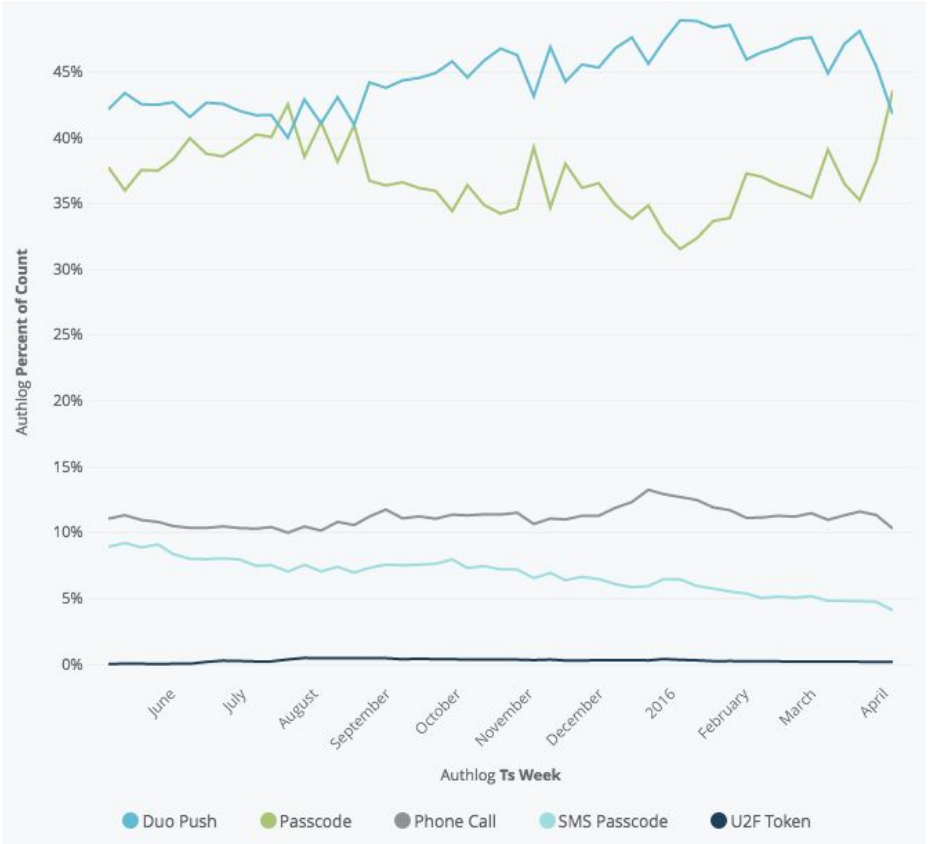
.

From bolt-on to built-in

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

Be patient...

- CrOS adoption
  - Hundreds of devices
- Windows 10
  - 15% of Win population
- U2F adoption
  - 1-2% of auths
- Ok, so it's very unevenly



Design for that future.

Design for the future

- Keep an open mind, think beyond the headlines
- Take action when go back this week
  - How do you simplify your security program?
  - Are you focusing on the fundamentals?
  - What's adding value and what's just creating work?
  - How are you designing for the future?
- Take that into your 2017 planning

Thank you!

Questions?

@jonoberheide
jono@duosecurity.com