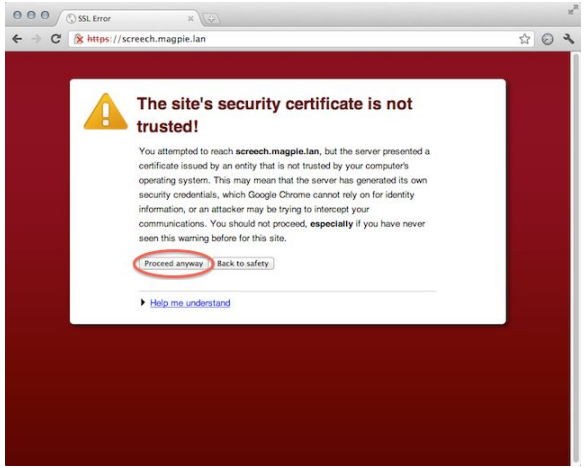
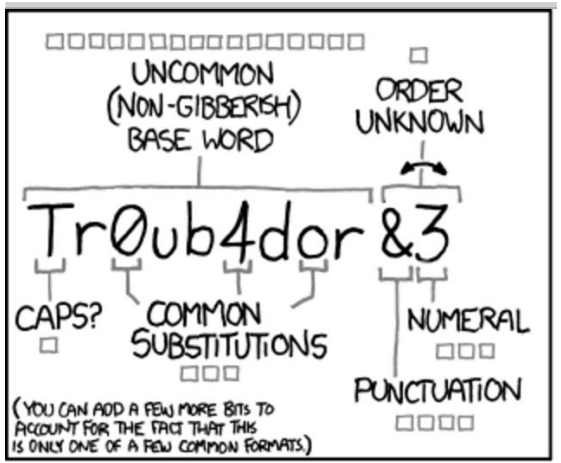
Security and Usability from the Frontlines of Enterprise IT

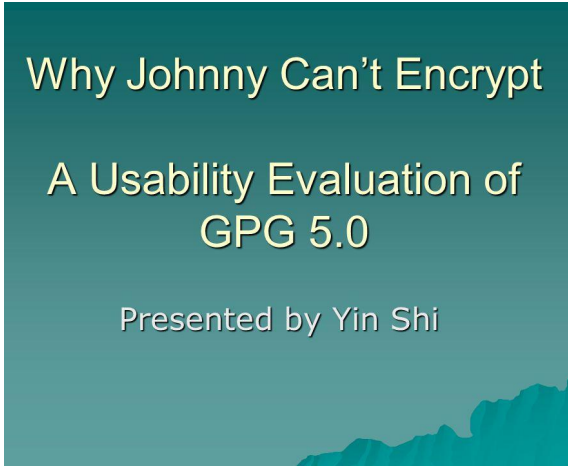
Jon Oberheide
CTO, Duo Security



Browser SSL warnings



Password schemes



Encryption usability

IT Security

40M consumer credit cards (direct)

153M end user credentials (indirect)

Thousands of affected orgs (meta)

VS.

Anthem

SONY

THE HOME DEPOT

TARGET

Security + Usability X The Industry Organizations Corp End Users X

duo.com

The Industry

Complexity
Sophistication
Advanced

>

Simplicity
Usability
Easy

This is BAD.


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

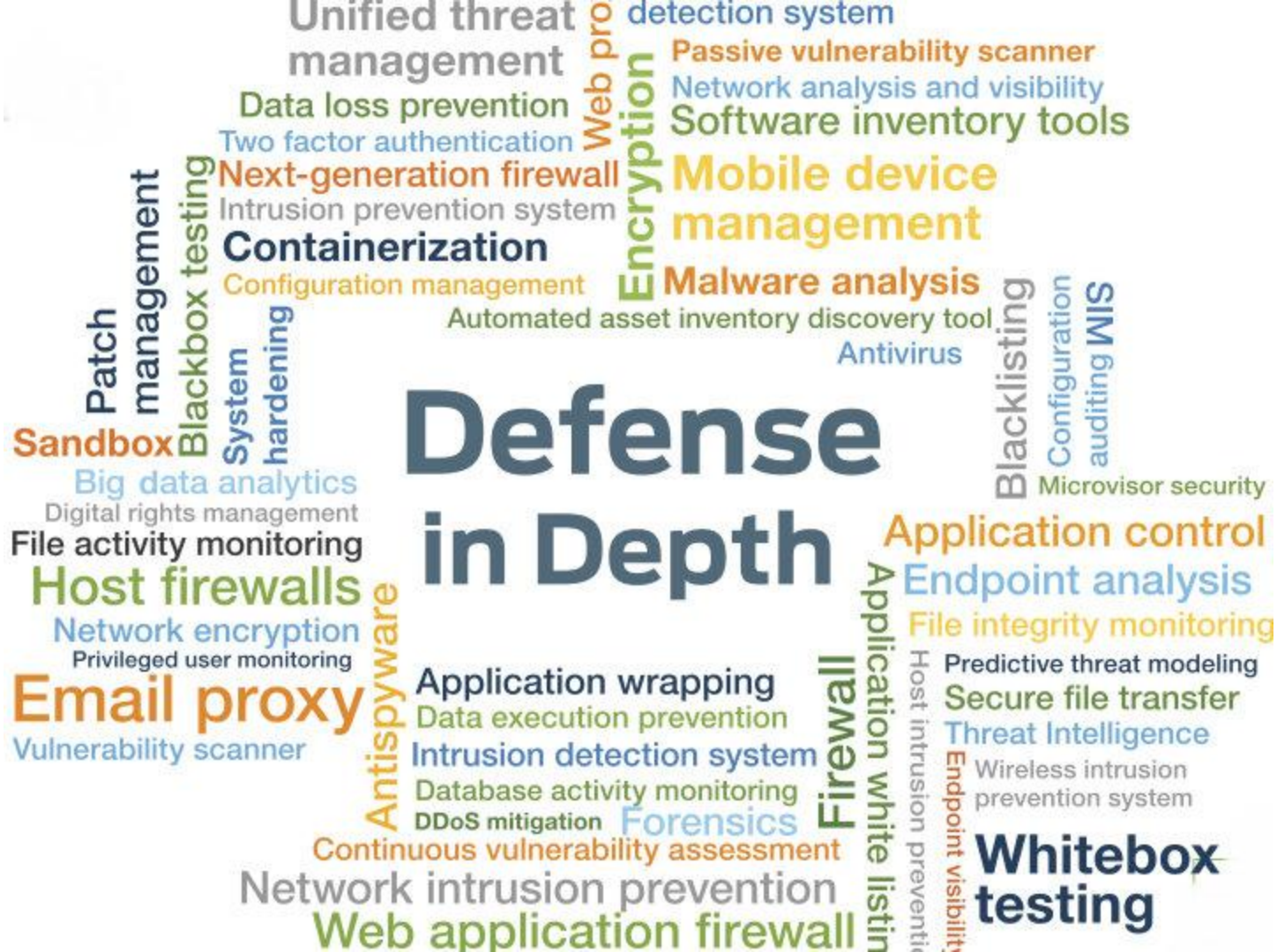

The Economist
Why fairness is a bad idea
Rewriting Wall Street's rules
Who will run Brazil?
How Big Oil became Big Gas
The link between IQ and disease
JULY 3RD–9TH 2010
Economist.com
Cyberwar
The threat from the internet
€5.50


VS.
SONY
PICTURES

Security and Usability from the Frontlines of Enterprise IT

Jon Oberheide, Co-Founder and CTO, Duo Security

When you think about security and usability, IT is probably
systems and security that underpin every organization are
employees, and the consumers they serve. At the same tim
market that requires a encyclopedic glossary to navigate, s
operationalize, and a user experience where "the users didn
sales pitch of "we suck less" is more effective that you mig
organizations demand more of their IT organizations and e
technology at work as they do at home. The bar is low for I


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

Figure 2 The Targeted-Attack Hierarchy Of Needs

107121

Source: Forrester Research, Inc.

1. Strong authentication
2. Up-to-date devices
3. Encryption

Confidentiality of data

Integrity of devices

Authentication of users

Basic security hygiene

What we should be doing:

What we're doing instead:

71%

of Android devices out of date

Android < 5.5.1, or < 6.0.1

75%

of OS X devices out of date

OS X < 10.11.2

50%

of iOS devices out of date

iOS < 9.2

START WITH SECURITY

The FTC's
Start with Security

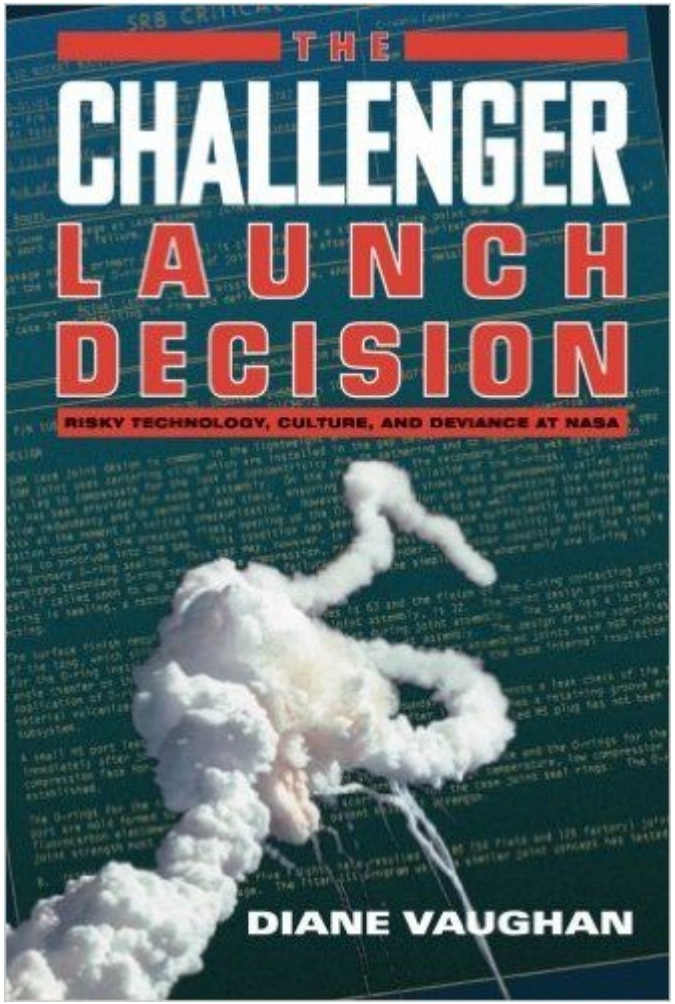
Google's
Beyond Corp

1. User auth-N, auth-Z
2. Device auth-N, auth-Z
3. Transport security

Organizations


IT 1.0: Mainframe
IT 2.0: Client/Server
IT 3.0: Cloud/Mobile

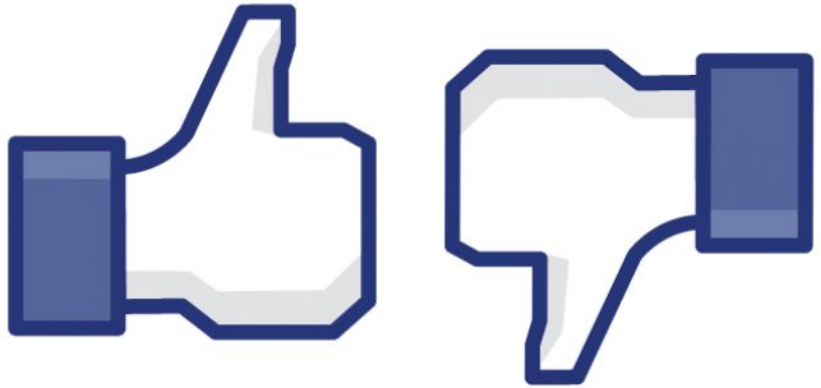
Dept of "NO" → Dept of Secure Enablement



*"Social **normalization of deviance** means that people within the organization become so much accustomed to a deviant behaviour that they don't consider it as deviant, despite the fact that they far exceed their own rules for the elementary safety."*

“With great power... →

… comes great
(shared) responsibility”



= Better security ?

Does usable IT security have an **indirect** positive impact for an org's security posture?

Do happy users have a **direct** positive impact on an org's security posture, either at a micro or macro scale?

End Users

“We should prefer security systems that people can readily create accurate mental models for, even if they are strictly less powerful than what the state of the art allows.”

-- Chris Palmer

Safety > Security

The coal gas story

United Kingdom suicide rates, 1960-71

NORMAN KREITMAN

cal Studies in Psychiatry, University Department of Psychiat
Edinburgh

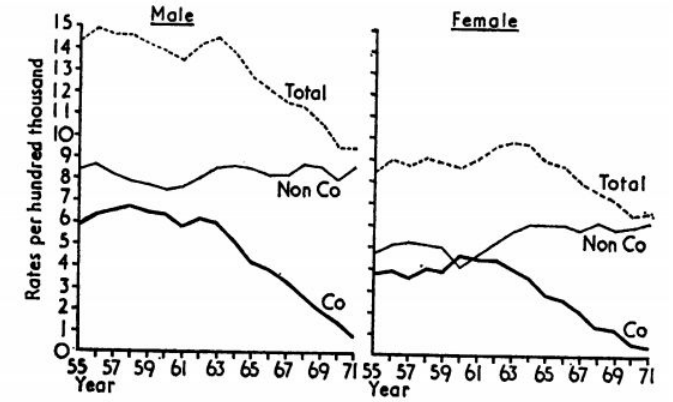


FIG. 4. England and Wales: sex-specific suicide rates by mode of death.

INSURANCE INSTITUTE
FOR HIGHWAY SAFETY

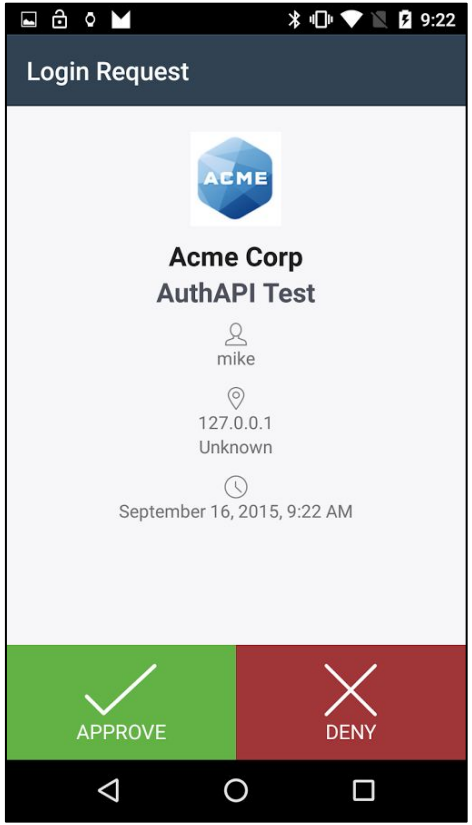
Safety > Security

Safe Behaviors > Technical Protections

“Tokens? Where we're going, we don't need tokens.”

Legacy 2FA

- Hardware tokens
  - Poor AX, UX
  - Expensive
- Phone call, SMS
  - Unreliable, insecure transports
- Software tokens
  - Countdown timer stress disorder
  - Symmetric key



Duo Push

- One-tap UX
- Strong transport security
- Asymmetric crypto

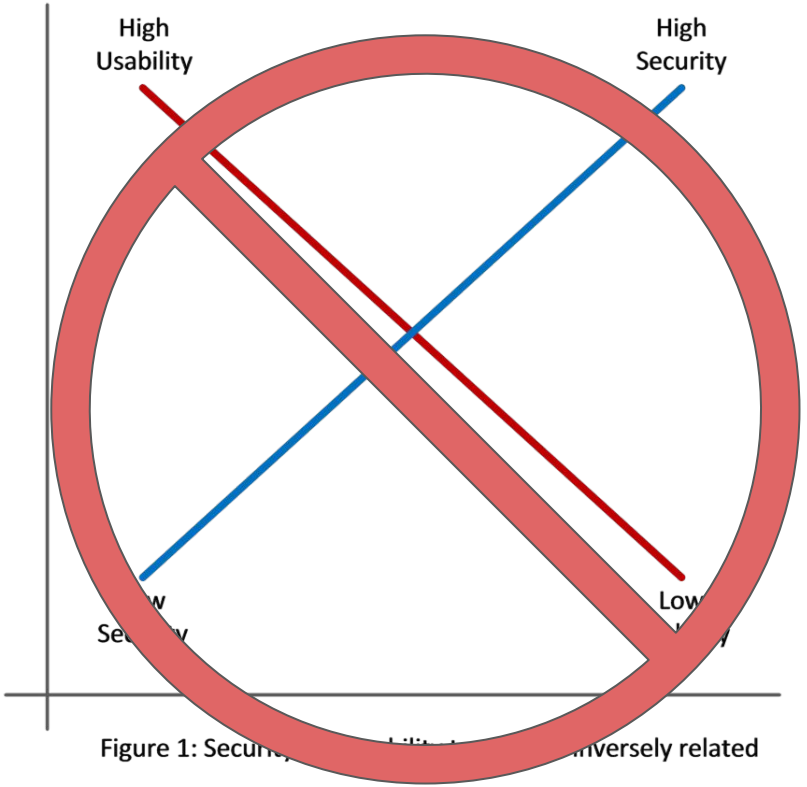
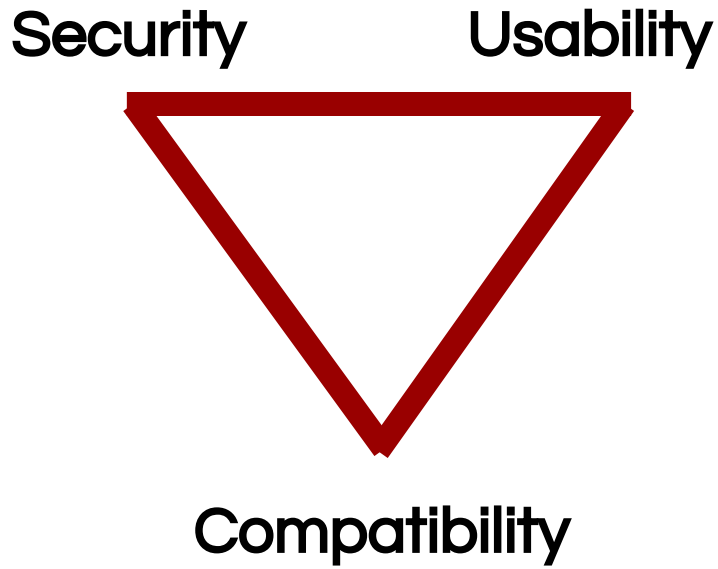
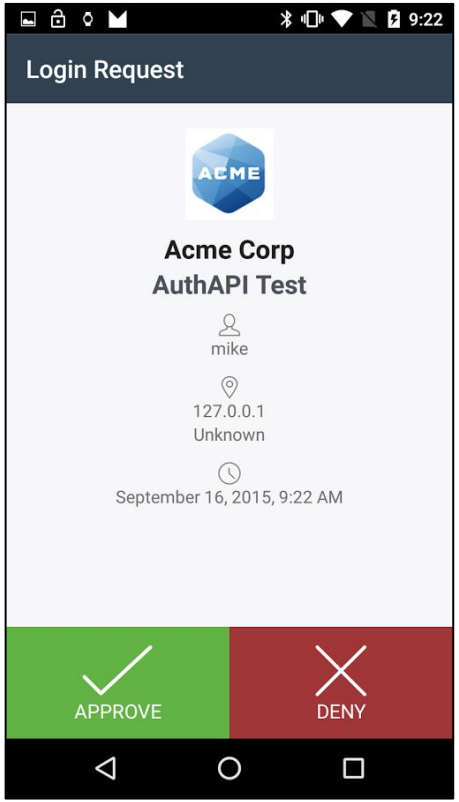
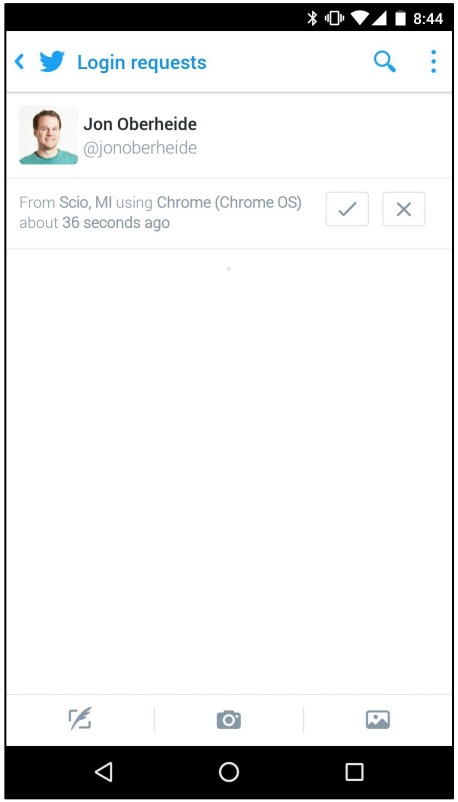


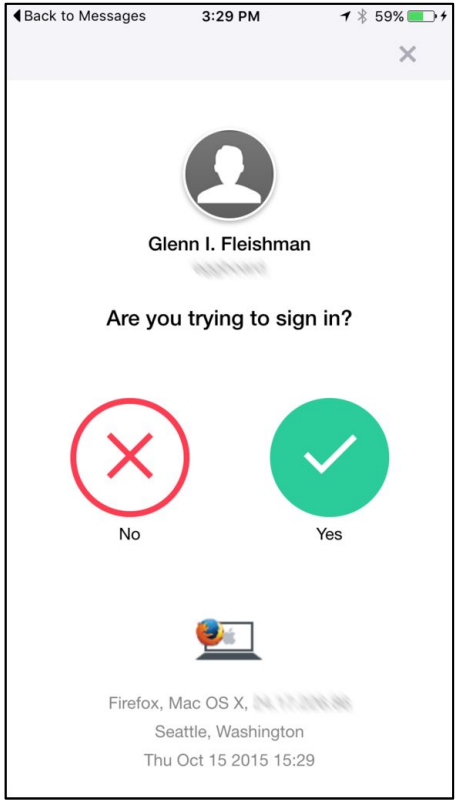
Figure 1: Secur iversely related

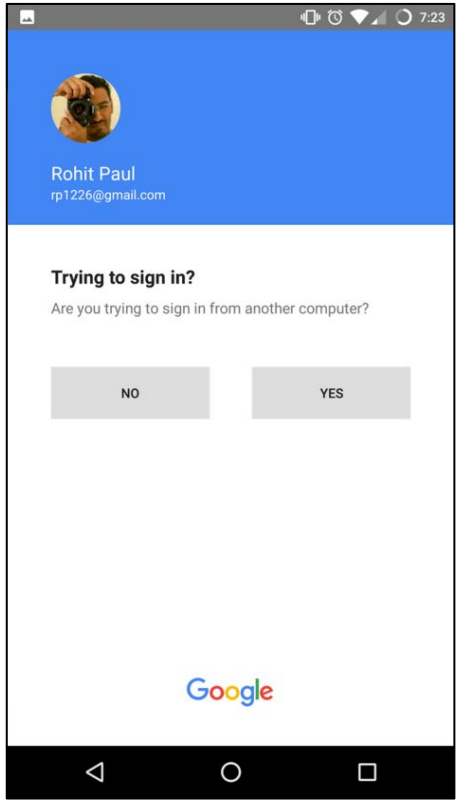


Note: Fulfills requirement of all presentations to have a Zooko Triangle









2010
[Duo Push]

2013
[Twitter]

2015
[Yahoo]

2016
[Google]

The Industry

Organizations

Corp End Users

jono's secret research agenda

- (S//SI//REL) Does usability and user happiness have a significant direct or indirect impact on IT security posture of an organization?
- (S//SI) At the corporate end user level
  - Are employees less susceptive to compromise or more likely to subvert IT security controls if they are perceived as usable and/or the users have a positive impression of their IT department?
- (S//SI) At an organizational level
  - Do usable security controls and happy users build organizational capital for IT? How much is user happiness or acceptance of security controls worth? How much does rejection of security controls cost an organization?
- (S//SI) At an industry level
  - Are positive models or architectures for IT security more effective or efficient?

Q&A

Jon Oberheide
CTO, Duo Security
jono@duosecurity.com
@jonoberheide

References

Slide 5:
- https://www.zerodium.com/ios9.html

Slide 11:
- http://blogs.forrester.com/rick_holland/14-05-20-introducing_forresters_targeted_attack_hierarchy_of_needs

Slide 12:
- http://blogs.forrester.com/rick_holland/14-05-20-introducing_forresters_targeted_attack_hierarchy_of_needs

Slide 13:
- http://blogs.forrester.com/rick_holland/14-05-20-introducing_forresters_targeted_attack_hierarchy_of_needs

Slide 14:
- Personal communication @ Google Security Summit 2015

Slide 16:
- Aggregate endpoint data from Duo's service on 2016/01/10

Slide 17:
- https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business
- https://www.usenix.org/conference/lisa13/enterprise-architecture-beyond-perimeter

Slide 20:
- http://dilbert.com/strip/2007-11-16
- Mike Kail

References

Slide 21:

- https://en.wikibooks.org/wiki/Professionalism/Diane_Vaughan_and_the_normalization_of_deviance
- https://www.schneier.com/blog/archives/2016/01/it_security_and.html

Slide 23:

- Personal communication with Ryan Huber @ Slack

Slide 24:

- http://publish.illinois.edu/science-of-security-lablet/science-of-human-circumvention-of-security/

Slide 26:

- https://noncombatant.org/2015/06/09/dubious-thoughts-crypto-usability/

Slide 28:

- http://www.ncbi.nlm.nih.gov/pmc/articles/PMC478945/

Slide 32:

- http://www.rlvision.com/blog/authentication-with-passwords-passphrases-implications-on-usability-and-security/

Slide 33:

- https://en.wikipedia.org/wiki/Zooko%27s_triangle

Slide 34:

- https://duo.com/blog/duo-push-the-next-generation-of-two-factor-authentication
- https://blog.twitter.com/2013/login-verification-on-twitter-for-iphone-and-android
- https://help.yahoo.com/kb/SLN25781.html
- http://techcrunch.com/2015/12/22/google-begins-testing-password-free-logins/