Security and Usability from the Frontlines of Enterprise IT

Jon Oberheide
CTO, Duo Security
Browser SSL warnings

Password schemes

Encryption usability

Why Johnny Can’t Encrypt
A Usability Evaluation of GPG 5.0
Presented by Yin Shi
IT Security
TARGET

40M consumer credit cards (direct)

Adobe

153M end user credentials (indirect)

Juniper Networks

Thousands of affected orgs (meta)
WANTED
REMOTE JAILBREAK FOR iOS 9

ZERODIUM.COM
$1,000,000.00 REWARD

VS.

Anthem

Sony

The Home Depot
Target
The Industry
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 time market that requires a encyclopedic glossary to navigate, sales pitch of "we suck less" is more effective that you might organizations demand more of their IT organizations and technology at work as they do at home. The bar is low for IT
Defense in Depth

- Unified threat management
- Passive vulnerability scanner
- Network analysis and visibility
- Software inventory tools
- Web proxy detection system
- Next-generation firewall
- Intrusion prevention system
- Containerization
- Mobile device management
- Malware analysis
- Automated asset inventory discovery tool
- Antivirus
- Big data analytics
- Digital rights management
- File activity monitoring
- Host firewalls
- Network encryption
- Privileged user monitoring
- Email proxy
- Antivirus scanner
- Application wrapping
- Data execution prevention
- Intrusion detection system
- Database activity monitoring
- DDoS mitigation
- Forensics
- Continuous vulnerability assessment
- Network intrusion prevention
- Web application firewall
- Application white listing
- Microvisor security
- Application control
- Endpoint analysis
- File integrity monitoring
- Predictive threat modeling
- Secure file transfer
- Threat Intelligence
- Wireless intrusion prevention system
- Whitebox testing
Expense in Depth
Figure 2 The Targeted-Attack Hierarchy Of Needs

- 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

Source: Forrester Research, Inc.
1. Strong authentication
2. Up-to-date devices
3. Encryption

C = Confidentiality of data
I = Integrity of devices
A = 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
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
MORDAC, THE PREVENTER OF INFORMATION SERVICES.

SECURITY IS MORE IMPORTANT THAN USABILITY.

IN A PERFECT WORLD, NO ONE WOULD BE ABLE TO USE anything.

To complete the log-in procedure, stare directly at the sun.

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 \textit{indirect} positive impact for an org’s security posture?

Do happy users have a \textit{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 Psychiatry, Edinburgh

Fig. 4. England and Wales: sex-specific suicide rates by mode of death.
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: Security and usability are inversely 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
(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 susceptible 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?
References

Slide 5:

Slide 11:

Slide 12:

Slide 13:

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.usenix.org/conference/lisa13/enterprise-architecture-beyond-perimeter

Slide 20:
- Mike Kail
References

Slide 21:
- https://www.schneier.com/blog/archives/2016/01/it_security_and.html

Slide 23:
- Personal communication with Ryan Huber @ Slack

Slide 24:

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:

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
- http://techcrunch.com/2015/12/22/google-begins-testing-password-free-logins/