National Institute of Standards and Technology
U.S. Department of Commerce

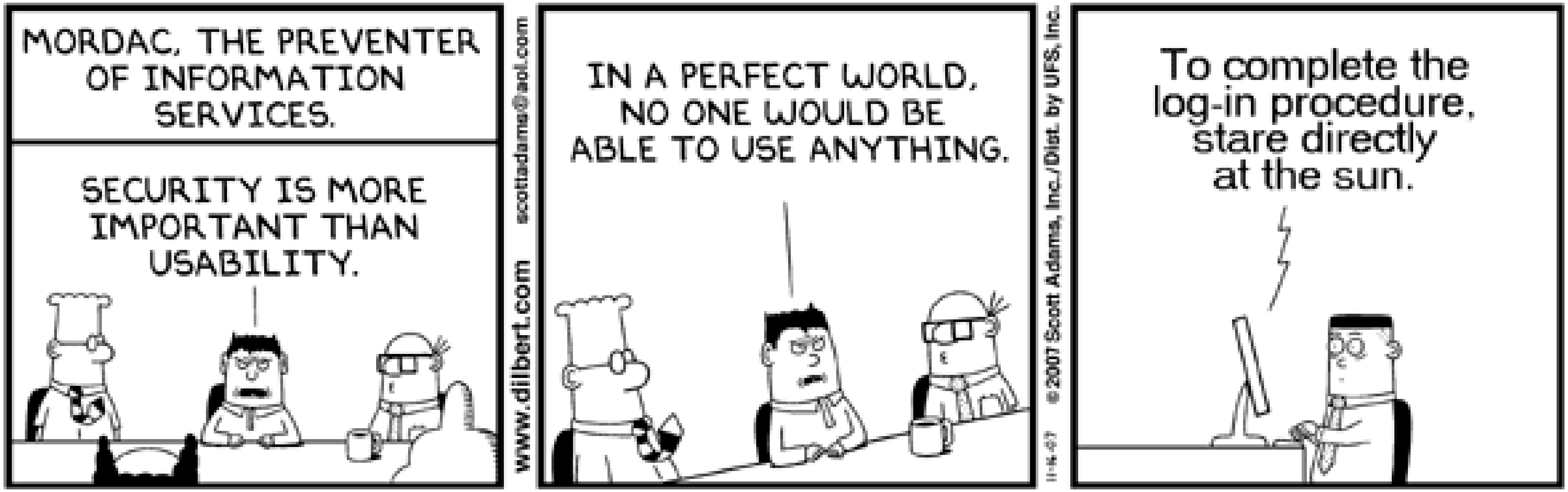
Information Access Division
Visualization and Usability Group

Usability and Key Management

Mary Theofanos

June 8, 2009

Biometrics and Usability


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

© Scott Adams, Inc./Dist. by UFS, Inc.

What makes it so hard?

- "Too many engineers consider cryptography to be a sort of magic security dust that they can sprinkle over their hardware or software,[…]"
- "Book after book explained cryptography as a pure mathematical ideal, unsullied by real-world constraints and realities."
- But it's exactly the real-world constraints and realities that mean the difference between the promise of cryptographic magic and the reality of digital security. "

Ferguson & Schneier in Practical Cryptography (2003)

A Reality Check: PKI Deployment for an Enterprise Wireless Network

Palo Alto Research Center (PARC)

- Idea was to give 200 users an X.509 certificate and to use 802.1x Extensible Authentication Protocol in TLS mode to authenticate to the wireless network
  - Request and retrieve certificates through web-based interface
  - Configure through GUI-based 802.1x configuration software
  - Administrators provided set of detailed instructions

And the result

Studied 8 users (Ph.D.s in Computer Science):

- Process involved 38 distinct steps
- Average time to request, receive certificate, and configure system 140 minutes
- Almost all followed the instructions mechanically
- Many described enrollment as most difficult computer task ever been asked to do
- All had little idea of what they had done to their machines
- Reduced their ability to configure and maintain their own machines.

One of those real-world realities is the Human Computer Interaction Thus the need for Usability

ISO 9241-11 defines usability as:

> “the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use”

First Tenet: Know Thy User

- Users’ characteristics: abilities and disabilities (accessibility)
- Users are task driven
    - Security is not their primary task
- Users will bypass security when it gets in the way of their primary task
- User perception influences behavior
    - Impossible demands
    - Need-value-benefit
    - Complexity
    - Lose respect for security
- Users’ understanding of security is weak

Mismatch in Conceptual Model

- Keys lock and unlock things
  - “keys” don’t sign things
  - “Keys” don’t authenticate things
  - Public and private keys – keys don’t generally work together (half a secret)
- Encryption is for secrets
- “Signature” indicates that it came from me
- What does certificate have to do with identity?

In general terms are misleading and overloaded

If I'm an end-user here's what I want to know:

- What problem are we trying to solve?
- What value/benefit does it provide to me?
- How does it make my life easier?
- Is it going to get in the way of getting my job done? – and how often?

Remember: Computer Security is not the user's primary goal!

Remember PARC Case Study

Usable PKI Deployment for Wireless Network

- Automated PKI and CA setup
- Enrollment Station is locked in room
  - Intuitive trust model
  - User and user's badge
  - Context of use
- Studies shows take 1minute 39 secs
- Total of 4 steps to add new device, retrieve certificate and install for use with the wireless network
- Positive user satisfaction and confidence

Systems are too complex

Let's examine certificates:

- "Acquiring a certificate is the single biggest hurdle faced by users" (Gutmann, Plug and Play PKI, 12th USENIX Security Symposium, 2003), Garfinkel & Miller Johnny 2 2005)
- UK eScience (Grid) Program, users complained about effort involved in obtaining and complexity of using certificates
  - Had to be stored in correct application directory
  - Many shared the certificate on that one machine
  - This important file was difficult to recognize
- We have conditioned users to ignore certificate messages and pop-ups

Do we really expect users to know all this?

1. How to import a trust anchor.
2. How to import a certificate.
3. How to protect your privates (private keys, that is).
4. How to apply for a certificate in your environment.
5. Why you shouldn't ignore PKI warnings.
6. How to interpret PKI error messages.
7. How to turn on digital signing.
8. How to install someone's public key in your address book.
9. How to get someone's public key.
10. How to export a certificate.

And a few more:

11. Risks of changing encryption keys.
12. How to interpret security icons in sundry browsers.
13. How to turn on encryption.
14. The difference between digital signatures and .signature files.
15. What happens if a key is revoked.
16. What does the little padlock *really* mean.
17. What does it mean to check the three boxes in Netscape/Mozilla?
18. What does "untrusted CA' mean in Netscape/Mozilla?
19. How to move and install certificates and private keys

The list for Developers and Administrators:

1. What does the little padlock *really* mean.
2. How to *properly* configure mod_ssl.
3. How to move and install certificates and private keys.
4. What .pem, .cer, .crt, .der, .p12, .p7s, .p7c, .p7m, etc mean.
5. How to reformat PKI files.
6. How to enable client authentication during mod_ssl configuration,
7. How to dump BER formatted ASN.1 stuff.
8. How to manually follow a certificate chain.
9. The risks of configuring SSL stuff such that it automatically starts during reboot.
10. How to extract certificates from PKCS7 files, etc

And a few more:

11. How to make PKCS12 files.
12. How to use the OpenSSL utilities.
13. What happens if a key is revoked.

Usability is more than the User Interface

1. Adopt mantra:

   Make it easy for users to do the right thing!

   - Definition of usability: users, goals, context of use
2. Align to the users conceptual model
   - Defining some of the terms on the interface differently
3. Reduce the complexity for the user
4. Address the certificate pop-ups
5. Eliminate those factors which inhibit adoption of new technologies and encourage those that factors that promote adoption

Shouldn’t usability of key management be an oxymoron?

References

- M. A. Sasse (2006): Has Johnny learnt to encrypt by now? Examining the troubled relationship between a security solution and its users. 5th Annual PKI R&D Workshop 2006
- N. Ferguson & B. Schneier (2003): Practical Cryptography. Wiley.
- P. Gutmann (2003)Plug-and-Play: A PKI your Mother can Use. Procs. 12th USENIX Security Symposium.
- S. Garfinkel & R.C. Miller (2005): Johnny 2: A user test key continuity with S/MIME and Outlook Express. Procs. SOUPS 2005.
- B. Leuf (2002): Peer to Peer: Collaboration and Sharing over the Internet. Addison-Wesley.
- D. Balfanz, G. Durfee, & D. K. Smetters (2005): Making the Impossible Easy: Usable PKI. Security and Usability. Eds. L.F. Cranor & S. Garfinkel. O'Reilly.