CyberWorld Intrusion Tolerance

Pankaj Goyal

Agenda

- Intrusion?
- Why Passwords
- Issues with Passwords
- Patches and Workarounds
- Intrusion Tolerance in an Online World

Intrusion and Impact

- Intrusion – unauthorized access
- Compromised Access
  - Physical world – keys or other entry points
  - Cyber world – ditto
- Impact
  - Physical world – break-in → theft, damage
  - Cyber world – squatting → theft, damage, and propogation

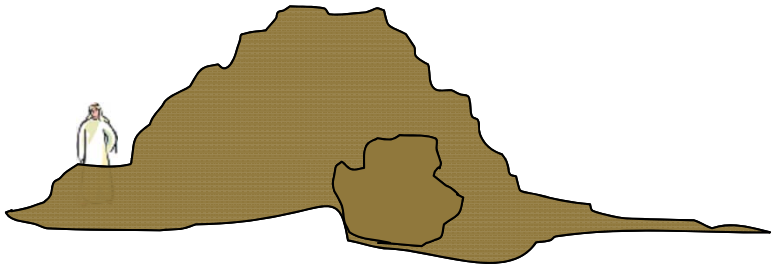
Cyber World Access

- Account – “address”
  - “address” = URL + Account Identity
- Account Identity
  - Mechanism to uniquely associate the account holder with an account
  - Verification?
    - ➢ authentication – prove who you claim to be

Authentication Choices

- What you know
  - Passwords (most common method)
  - Challenge Questions
- What you have
  - Credentials (can be Identification), smart-cards, mobile devices, Keys
- What you are
  - Biometrics

Vulnerability – Eavesdropping

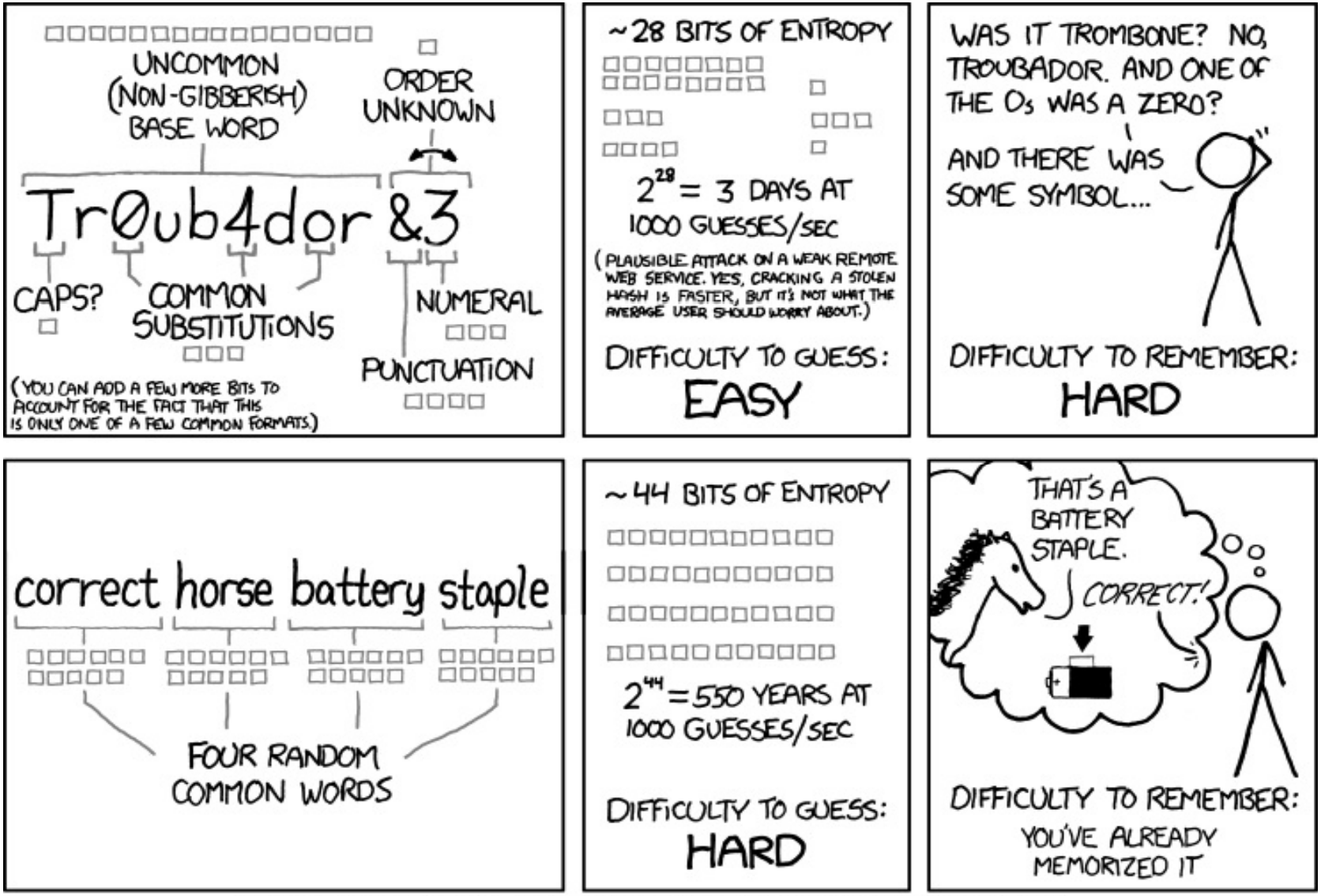


The First Hacked Site – Robber's Cave

Shared Password "Open Seasame"

Why Passwords

- History of Use
  - “entry” (Identity a non-issue)
  - Document, Seal etc
- Part of childhood games
- Ease of Use
- Easy to Replace/Recover (for User)
- Ubiquitous Applicability



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Just Some 2011 Incidents

- Sony Playstation – 101 million
- Epsilon (Walt Disney, JPMorgan Chase, Best Buy – 60 million
- Wordpress – 18 million
- Booz Allen Hamilton (DoD) – 90,000
- NATO – 11,000 (e-Bookshop)
- Expedia – undisclosed (likely huge)
- RSA (secure-ID; 2-factor) – ???

Password Issues

- Memorizable passwords – easy and few
- Password Reuse across systems
  - Reuse rates increase over time
  - Sharing passwords is a sign of trust
  - Unique passwords – majority users < 5
  - Variable System Security
- Challenge Questions
  - 34% asked for a human name, 15% asked for a pet name and 20% asked for a place name
  - Social Media Mining – U have > 2K friends!!!

Alternatives

- Smart Cards
- Biometrics
  - Finger prints
  - Facial Recognition
- PDA/Smart Phones
- Multi-factor (2-) authentication
  - Users consider passwords to be safer

Issues with Alternatives

- Deployment – infrastructure, scalability, …
- Replacement
- Disablement of lost
- Non-ubiquitous (specific applicability)
- Foolproof ??
  - Theft, Counterfeit, Denial of Access
  - Man In The Middle attacks
  - Can U trust other party

Vulnerability – Patches & Workarounds

- Password/Credential Loss
  - Replacement, Recovery (use informed)
- Password Vaults
  - Store “strong” passwords
  - Loose Vault password …..
- Password Generators
  - Generate “strong” passwords
  - Current systems have major usability issues

Do Not Address Attack Scenarios

Impact of Compromised Access

- Recovery – unintended consequences
  - Challenge Questions allow access and password change
- Compromised Access
  - Systems inform on password change
  - Profile change – email, phone, address, ..???
- OTP – out-of-band channel
  - Users required to copy authorization code
  - Users unable to identify minor changes

So What Are We To Do

ReBoot

- Objective
  - Assume intrusion
  - Prevent/Minimize “Loss”
  - Assess End-2-End Process Vulnerabilities
    - Profile changes – Self, “Beneficiaries”
    - Transactions
  - Utilize Available Communication Channels
    - Simultaneous multi-modal interactions

Intrusion Tolerance Policy (examples)

- User Authorizations thru auxiliary channel
  - Acceptable interaction & auxiliary channels (allow user selections within defined sets)
- Profile, Activity and Transaction changes
  - Pending status (effectively inactive) until Authorized (allow user set limits)
- Encryption
  - User-Id, Password, Personal Id Info, Profile, Transaction/Activity Id
- Challenge questions only psychological

Impacts of Policy

- Interaction channel compromise
  - Specified compatible auxiliary channels
  - Authorizations from auxiliary channel
- Changes
  - Add/modify beneficiary – authorization
  - Add/modify transactions – authorization

Remarks

- Intrusions will occur
- Time for a rethink
- Start from Basics
  - Objectives
  - E2e processes
    - ➢ Assess Vulnerability – a la lean and values
    - ➢ Address single point of failures

Some References

- M. AlZomai, et al., “An Experimental Investigation of the Usability of Transaction Authorization in Online Bank Security Systems,” 6th Australasian Conf Inf Security, 65-73, 2008
- E. Felton, et al., “Web Spoofing: An Internet Con Game,” 20th Natl Inf Sys Security Conf, also TR 540-96, Princeton University, 1997, http://www.princeton.edu/sip/pub/**spoofing**.html.
- S. Gaw, E.W. Felton, “Password management strategies for online accounts,” SOUPS '06 2nd symp on Usable privacy and security, 44-55, 2006
- J.A. Halderman, et al, “A Convenient Method for Securely Managing Passwords,” 14th Intl Conf WWW’05, 471-479, 2005
- C. Herley, et al., “Passwords: If We're So Smart, Why Are We Still Using Them?” Financial Cryptography and Security, 230-237, 2009.
- J. Kelsey, et al, “Secure applications of low-entropy keys,” *LNCS*1396:121–134, 1998
- B. Ross, et al, “A browser plug-in solution to the unique password problem,” 2005. Stanford-SecLab-TR-2005-1.
- S. Singh, A. et al., “Password Sharing: Implications for Security Design Based on Social Practice,” SIGCHI conf Human factors in comp sys (CHI ’07), 895–904, 2007
- C.S. Weir, et al., “Usable security: User preferences for authentication methods in eBanking and the effects of experience,” Interacting with Computers, 22 (3), 153-164, 2010

General References

- R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Ed, Wiley Publishing, 2008
- J. Bonneau, S. Preibusch, “The password thicket: technical and market failures in Human authentication on the web,” 9th Workshop Econ Inf Security, 2010