Beyond “usable security”

Arash Habibi Lashkari
Nottingham – Malaysia
March 2012

Overview

- A brief history of “usable security”
- Why usable is not enough
- Key elements of designing effective security
  - White Paper on Human Vulerability in Security

Background

- Study on password problems at BT Labs
- Too many passwords
- Too many password changes

"Why Johnny can't encrypt"

- Whitten & Tygar, *Procs USENIX 1999*
- Graphical user interface to PGP 5.0
- Even after detailed introduction, only 3 out of 12 participants could encrypt their email successfully
- Need more than a pretty face: graphical ≠ usable
- Problems:
  1. User tasks not represented in UI
  2. Misleading labels
  3. Lack of feedback

Human-Computer Interaction

general & specific characteristics

USER  ***SYSTEM***

interacts with

to attain

GOAL

MH & xmh

by carrying out **TASK**

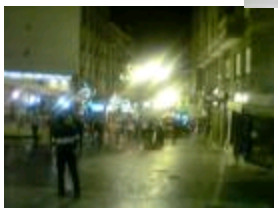
interaction takes place in a

CONTEXT

physical 

social 

cultural 

temporal 

General User Characteristic: Human Memory

- Limited capacity
- Decays over time (items cannot be recalled at all or not 100% correct)
- Frequent recall improves memorability
- Unaided recall is harder than recognition
- Non-meaningful items much harder to recall than meaningful ones
- Similar items are easily confused
- Items linger - cannot “forget on demand”

Password Systems

- Require unaided recall
- Entry must be entered 100% correct
- Not meaningful (no words, names, phrases)
- Many similar items compete
  - Frequently change
  - Proliferation of items that users have to recall (banking, phones, websites)

Users cannot cope – so …

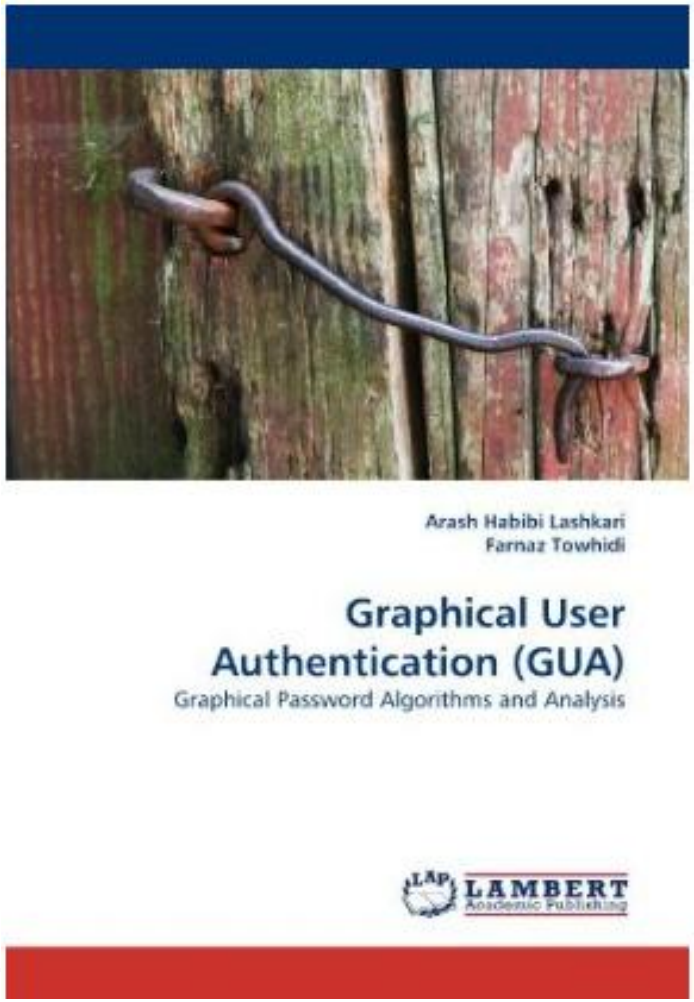
Further insights

- Most people struggle even more with PINs than with passwords
- Majority of people write down all or some of their passwords and PINs
- Passwords and PINs chosen by people are vulnerable to cracking and guessing attacks
- Conflicting requirements of *production task* and *security task*

Importance of task and performance

- Passfaces trial
- Good memorability, but too slow for regular logins
- Decreased usage of system by 60%
- Increased user satisfaction by 70%
- Increase memorability, by 80%

Graphical Passwords (GP)
Graphical User Authentication (GUA)



Graphical User Authentication (GUA) has two symbiotic pillars as its foundation: USABILITY & SECURITY.
The macro-concept of GUA is based on the human psychological factor that is images are more readily committed to memory than would TBPA's. All GUA algorithms are made up of both usability and security aspects.

This book tries to find and explain GUA algorithms from 1996 till 2010 and define the evaluation features of GUA algorithms based on standards. Finally the GUA algorithms will be evaluated by these evaluation methods.

Arash Habibi Lashkari - 2010

Jakob Nielsen's Alertbox November 26, 2000

"In future, security [and usability] will improve through biometrics such as fingerprint and retina scanning (though fingerprints don't work for some people."

BBC NEWS UK EDITION

Last Updated: Wednesday, 17 September, 2003, 08:38 GMT 09

E-mail this to a friend Printable version

Eye scan school opens doors

A £14m Sunderland secondary school opens its doors to pupils on Wednesday, after a delay of a week and a half.

The Venerable Bede Church of England school should have opened on 8 September but building works also overshot a second opening date last Friday.

The system will be used for ordering school dinners

Staff and governors at the so-called "super school" have said that the best is worth waiting for with a building and facilities fit for the 21st century.

BBC NEWS UK EDITION

Last Updated: Monday, 13 September, 2004, 15:29 GMT 16:29

E-mail this to a friend Printable version

Eye scanner project is scrapped

A Wearside school which became the first in Europe to use a futuristic eye-scanner has scrapped the scheme because it was too slow.

The eye scanner has been scrapped for being too slow

Venerable Bede Church of England School in Ryhope, Sunderland, introduced the hi-tech system to take away the stigma felt by pupils entitled to free meals.

The scanner was able to identify pupils anonymously by taking a picture of their eyes.

But the scheme has now been replaced by swipe cards because it was too slow.

"We were aiming for it to scan 12 pupils a minute, but it was only managing 5 so has been temporarily suspended as we do not want pupils' meals getting cold while they wait in the queue."

It’s the requirements, stupid!

“Non-security experts have security requirements, but cannot express them.”

Dieter Gollmann – Computer Security

What do you mean, human vulnerabilities?

"Security is a chain, and people are the weakest link in the chain."

Security guru **Bruce Schneier**,

Secrets and Lies 2000

The Problem Space

Background

Extensive use of ICT, coupled with speed of change → knowledge and skills gap

Globalisation, pressure to be profitable: outsourcing and offshoring → deperimeterisation of security → security models based on systems, perimeters, command-and control don't work

Security:

Security implemented with insufficient consideration of impact on users

→ high workload, complexity and bypassing of security mechanisms

→ lack of understanding what drives human behaviour

Cyber Security
Knowledge Transfer Network

What can be done? Design

Participative approach to security analysis and design

Most stakeholders have security requirements – just ask simple questions they can understand

Don't add it on, design it in!

Put security requirements into spec, don't treat them as NON-FUNCTIONAL

Security must not strangle business process

Even better: get additional value out of security measures

Removing opportunities, reduce possible rewards

Criminology, psychology, economics

What can be done - Awareness, Education and Training

Currently badly understood & executed

Awareness

Raising interest and attention

Education

Knowledge about risk, relationship between own behaviour and security

Training

Breaking old habits and establishing new ones

Based in the work context and addressing specific security needs

Cyber Security
Knowledge Transfer Network

Managing Organisational Behaviour

Human behaviour in the workplace

Areas with commonality: Productivity, job satisfaction, staff turnover, absenteeism…

Gap between formal security policies and procedures and actual behaviours needed

Organisational Citizenship Behaviour (OCB)

Managed through psychological contracts

Based on *concordance* (not command-and-control)

Conclusions

- Most people like to believe that technology is the answer to their security problems.
- *“If you believe that, you don’t understand security or technology.”* Bruce Schneier
- Security isn’t that special – application of usability/design knowledge and methods solves most problems
- Don’t focus on UIs to security tools – the big problems are in security requirements, job design and user involvement