

SECURITY AND USABILITY

AN INTRODUCTION

Kjell Førgen Hole

NoWires Research Group
Department of informatics
University of Bergen

Last updated October 20, 2008

Outline

- * Security and usability fundamentals
- * Usable and secure authentication mechanisms
- * Poor TLS/SSL usability reduces security
- * Extended Validation (EV) certificates
- * Design principles for usable security

FUNDAMENTALS

Information systems and risk

- * An **information system** consists of computers, communication networks, and storage equipment
- * A **risk** associated with an information system is a possibility that a user, or some other stakeholder, will experience a negative outcome attributable to the system
- * the risk is a function of the system's relevant vulnerabilities, threats, and assets
- * risk is a subjective quantity in practice

Security and usability defined

- * **Security** is the process of keeping the risks of an information system at a level acceptable to all stakeholders
- * The **usability** of an information system denotes the ease with which users are able to utilize the system to achieve their goals

Usability gone wrong



5

Fundamental trade-off?

- * Security and usability of an information system are non-functional requirements in software engineering terms
- * The need for security and usability is often not considered until the design of a system is (nearly) completed
- * **Observation 1:** As a result, many practitioners have come to believe that there is a fundamental trade-off between achieving satisfactory security and usability

6

S&U observations (1)

- * The usability of a security mechanism depends on both the users and the environment in which the mechanism is used
- * Usability is *not* achieved when developers design a security mechanism to meet their own specifications
- * mechanism must satisfy regular users' needs

7

S&U observations (2)

- * Usability is often the weakest link in the security chain of an information system
- * **Observation 2:** Poor usability can cause serious exploitable vulnerabilities and, thus, significantly reduce the security
- * As we shall see, SSL/TLS is an example of this problem

8

USABLE AND SECURE AUTHENTICATION



Authentication defined

- * An **identifier** points to an individual. An identifier can be a (personal) name, a serial number, or some other pointer to the individual being identified
- * Individual authentication, or just **authentication**, is the process of establishing that an identifier refers to a specific individual
- * Very often, a user submits a name, the identifier, and a secret password during the authentication process

Limitations of password-based authentication

- * Because of human information processing limitations
 - * users write passwords down
 - * users share passwords with other users
 - * users choose passwords that are memorable but not secure
 - * users forget passwords
- * As a result, “traditional” password-based authentication techniques are weak and have limited usability

11

Techniques to reduce memory demands (1)

1. Keep the number of password changes to a minimum
 - * login failures increase sharply after password changes
2. Provide password mechanisms that are forgiving
 - * most users do not completely forget passwords
 - * they tend to confuse passwords, not recall them 100%, or mistype them
 - * a large number of trials reduces number of failed logins significantly

12

Techniques to reduce memory demands (2)

3. Provide mechanisms that require users to recognize items rather than recall them

(I) *recognition of images*

(II) *text-based challenge-response mechanisms*

* **Observation 3:** Security experts tend to reject suggestions that improves usability, because attackers may get extra help

13

(I) Authentication based on image recognition

* **Graphical authentication** is interesting because

- a. pictures are more easily remembered than words
- b. visual memory seems not to be significantly affected by the general decline of cognitive capabilities associated with aging
- c. modern PCs have good graphical capabilities

* the same is not always true for mobile phones

14

Graphical authentication approaches

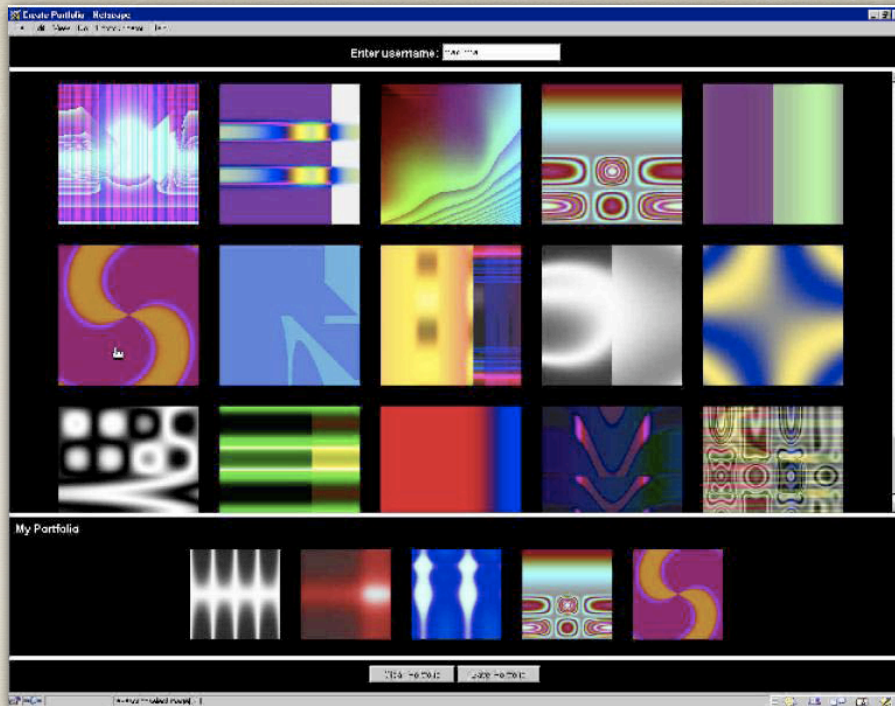
- * Graphical authentication techniques can be divided into two main approaches
 - a. *Recognition-based techniques*—user selects target pictures among a set of distractors
 - b. *Position-based techniques*—user identifies target objects within a picture

15

Graphical “password” examples

- * Select images that together constitute a “password” from among many pictures of
 - * abstract images
 - * everyday objects
- * Must be able to stop automated searches for the correct “password” because the search space is small
- * **Observation 4:** Closing of user accounts enables (D)DoS attacks at the application layer

16



Example of graphical authentication where user chooses a small number of preselected pictures

17



* Example where a user recognizes three objects and click inside the triangle defined by the objects

18

Drawbacks

- * Time-consuming authentication
- * Excludes blind users
- * It is not known how hard it is to crack graphical passwords
- * Large-scale user trials needed
- * vulnerable to (D)DoS attacks?
- * **Observation 5:** Graphical authentication techniques are still immature. More work is needed to better understand their potential

19

(II) Authentication with challenge questions

- * The authentication process requires the user to answer certain questions
 - * **Question:** What is a memorable date for you?
Hint: Dog
- * Necessary to ask multiple questions

20

Disadvantages

- * It is difficult to determine questions attackers cannot find or guess the answers to
- * Difficult to construct a system that scale well, i.e., asks the right questions to a large number of users
- * The authentication is time consuming because multiple question-answer pairs must be used
- * **Observation 6:** Authentication with questions seems less promising than graphical authentication

21

POOR TLS/SSL
USABILITY

TLS/SSL and phishing

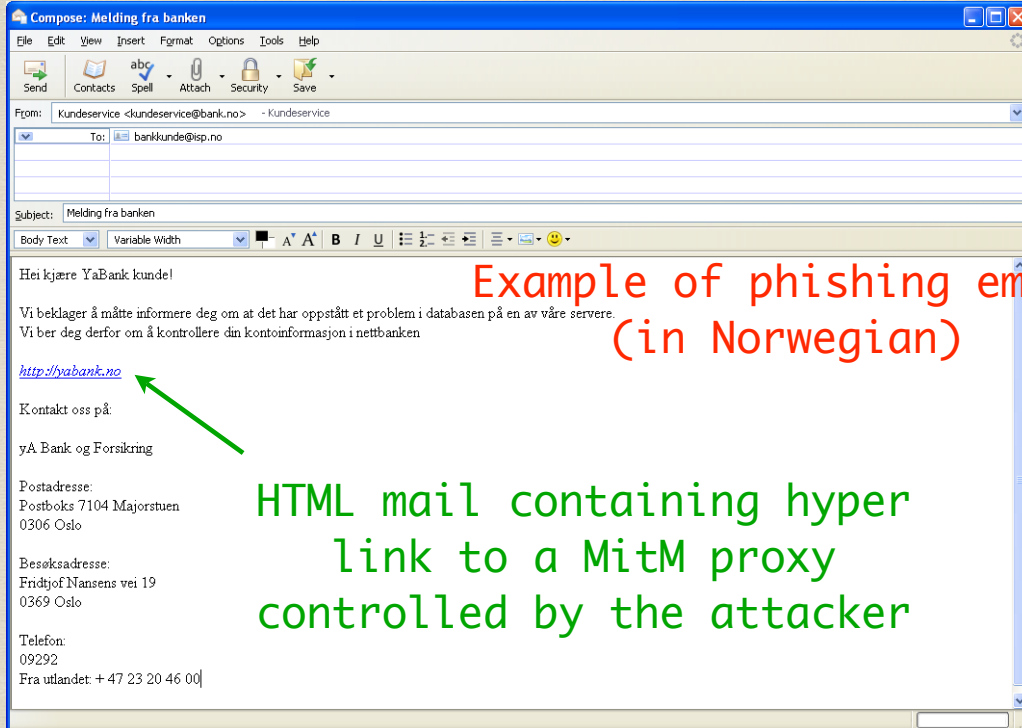
- * TLS/SSL is supposed to provide strong server authentication in client-server systems
- * The cryptography in TLS/SSL is theoretically strong, but, as we shall see, poor usability still results in weak authentication in practice
- * TLS/SSL cannot prevent **phishing attacks**, i.e., a combination of social engineering and Man-in-the-Middle (MitM) attacks

23

Typical phishing attack (1)

- I. Attacker sends phishing email to a victim asking him or her to log on to a fake web site masquerading as a genuine site
 - * the email contains an embedded hyperlink pointing to the fake web site
 - * the email typically describes some problem and asks the user to log on to rectify the problem or verify that the problem has been solved by the owner of the genuine site

24



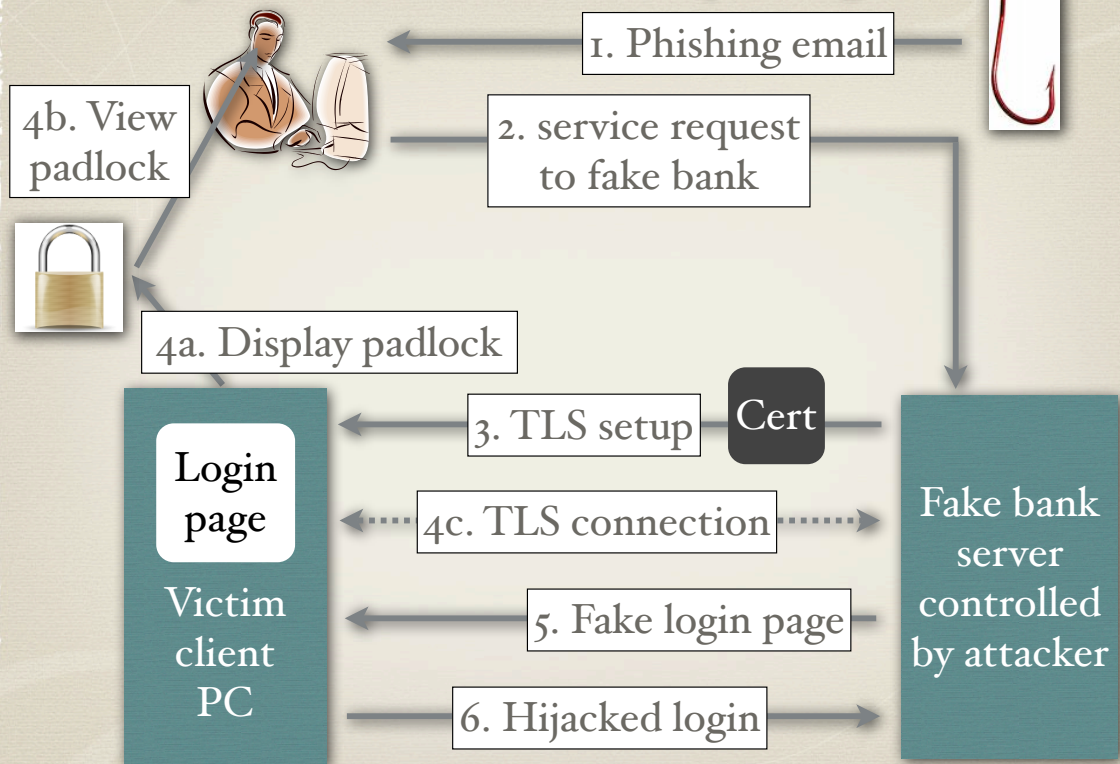
25

Typical phishing attack (2)

2. Users are tricked into logging on to the fake web site because the attacker has copied images and page designs to make the fake site look just like the legitimate site
 3. After the attacker has obtained the victim's login credentials, he logs on to the genuine web site, passing himself of as a legitimate user
- * alternatively, the victim may be tricked into disclosing sensitive personal or financial information that the attacker can use for financial gain later on

26

Phishing attack on online bank exploiting TLS



Phishing details

- * Studies have shown that between 1 to 3 percent of the people receiving phishing emails enter their login credentials at a fake web site
- * Different phishing attacks are possible. In some instances, it may be possible to exploit design or implementation weaknesses to simplify an attack

Attack analysis: not a technical problem

- * Technically speaking, the fake site has been correctly authenticated if it uses TLS/SSL, since the fake site is in fact claiming its own identity
- * Unfortunately, the victim has confused the fake site with a legitimate site

29

A usability problem: the padlock

- * The current web browsers display a picture of closed padlock to indicate that TLS/SSL is active
- * alas, the padlock does not provide any identity information about the server
- * furthermore, a web page may display a fake padlock by simply including a picture in the correct position on the page

30

A usability problem: the server certificate

- * Additional identity information is provided by a server certificate that the user can inspect by double-clicking on the padlock
- * Experience has shown that the information in the certificate is hard to understand for many users
- * Hence, a user may not detect that he is seeing a certificate from a fake web site instead of the certificate from the legitimate site

31

Study of server certificate

- * The attacker has obtained a public-key certificate containing an URL similar to the URL of the legitimate site
- * The certificate is installed on the fake server

32

URLs and HTTPS

- * If the URL of the fake web site and the URL of the legitimate site are nearly equal, then the user may not spot that he is communicating with the fake site
- * `https://www.nowires.org` (original)
- * `https://www.n0wires.org` (fake)
- * `https://www.nowiires.org` (fake)
- * It is not difficult to generate a self-signed certificate to support https

33

Correct URL?

- * How can a user verify that the following URL (belonging to a Canadian online bank) is correct?
- * `https://www.txn.banking.pcfincial.ca/a/authentication/preSignOn.ams?referid=loginBox_banking_go`
- * To make problems worse, the URL in the certificate belonging to the legitimate cite may not match the URL of the actual login page

34

(1) The crux of the problem

- * On one hand, URLs are designed for Internet applications and provide poor usability for naming real organizations like banks
- * On the other hand, ordinary names are suitable for real organizations, but not for online authentication
- * As a result, the users do not know which service provider identity to expect when accessing online services, and authentication becomes meaningless

35

(2) The crux of the problem

- * Investigations show that many users
 - * do not check URLs at all
 - * do not understand the significance of the extra 's' in https
 - * do not look for the padlock icon

36

EXTENDED VALIDATION

Improving trust through enhanced procedures for certificate issuing and validation

Legal accountability needed

- * TLS with X.509 v3 certificates from many CAs only validates domain names
- * **Legal accountability** requires more information:
 - * Proof that the applicant has the right to apply for the certificate on behalf of the subject
 - * Proof that the entity described in the subject name is legally registered according to the (local) law
 - * A verified address where legal process can be served

Extended validation certificates

- * The CA/Browser Forum has developed guidelines
 - * for issuing Extended Validation (**EV**) certificates (special type of X.509 certificates)
 - * for verifying and ensuring the legal identity of the certificate holder
- * Enhanced Internet browsers (IE, Firefox, Opera) offer a more user-friendly validation of EV certificates

39

USABLE SECURITY

When users fail to comply with the behavior required by a secure system, security will not work as intended

Current situation

- * An increasing number of companies suffer security incidents, partly because
 - * users fail to utilize security mechanisms such as virus checkers and email encryption correctly
 - * Users fail to show the required behavior because they
 1. are unable to behave as required
 2. do not want to behave as required

41

Security and usability requirements

- * A security mechanism must be designed for ease of use, so that users routinely and automatically apply the mechanism correctly
- * The users' mental model of the security goal must match the implemented security mechanism

42

Need for design principles

- * User-centered design principles are needed to develop mechanisms that are
 - * understood and utilized by all users
 - * support the users' main goals
- * These design principles must take into account that security is not the users' main goal when utilizing an information system

43

1. Design principle

- * Users want security controls to be as transparent as possible
- * On the the other hand, they want to be in control and understand what is happening

Security mechanisms need to be accessible to users, but should not get in the way of the users' main goals

44

2. Design principle

- * The users must accept the security mechanisms to avoid their inclination to circumvent the security
- * If a security solution is too complex, then users will not understand it and costly errors will occur

It must be easy for users to understand the need for security

45

Need for better development techniques

- * The suggested design principles must be incorporated into current development techniques
- * In addition, usability testing with real users—not the designers and implementors—is crucial to obtaining both adequate usability and security
- * **Observation 7:** Many development techniques do not take security and usability into account at all

46

CONCLUSIONS

Conclusions

- * Graphical authentication has the potential to overcome some of the problems associated with text-based authentication
- * However, more research is needed before graphical authentication can be applied in sensitive systems such as online banks
- * A new usable alternative to TLS/SSL is needed
- * New development methodologies are needed that take both usability and security into account from the start

(1) References

1. L. F. Cranor And S. Garfinkel, Editors, *Security and Usability*. O'Reilly, 2005.
2. X. Suo, Y. Zhu, and G. S. Owen, "Graphical Passwords: A Survey," in proc. *Twenty-First Annual Computer Security Applications Conference (ACSAC)*, Tucson, Arizona, USA, Dec. 5-9, 2005.

* www.acsac.org/2005/papers/89.pdf

(2) References

3. A. Jøsang, B. AlFayyadh, T. Grandison, M. AlZomai, and J. McNamara, "Security Usability for Vulnerability Analysis and Risk Assessment," in proc. *Twenty-Third Annual Computer Security Applications Conference (ACSAC)*, Miami Beach, FL, USA, Dec. 10-14, 2007.

* www.acsac.org/2007/papers/45.pdf

4. M. Mannan and P. C. van Oorschot, "Security and Usability: The Gap in Real-World Online Banking," in proc. *New Security Paradigms Workshop 2007 (NSPW07)*, North Conway, New Hampshire, USA, Sep. 18-21, 2007.

(3) References

5. P. Hallam-Baker, *DotCrime Manifesto*. Addison-Wesley, 2008
6. CA/Browser Forum, www.cabforum.org