

# Security Usability Principles for Vulnerability Analysis and Risk Assessment

Audun Josang  
Faculty of Information  
Technology, QUT

Bander AlFayyadh  
Information Security  
Institute, QUT

Tyrone Grandison  
IBM Almaden Research  
Center

Mohammed AlZomai  
Information Security Institute, QUT

Judith McNamara  
Faculty of Law, QUT

# Talk Outline

- Motivation & Background (MB)
  - Security and Usability
  - Risk Assessments
- Implications of Current Landscape
- Our Contribution
- Usable Security Approaches
- Principles of Security Usability
- Usability and Risk Assessment
- Demonstrating Value
  - Case Study: Web Security Usability
  - Case Study: Transaction Authorization Usability
- Conclusion

# MB: Security & Usability

- The state of affairs for security systems
  - Systems are built to defend against adverse impacts.
  - The strength of a security system is determined by its weakest link.
  - In the majority of cases, the human operator is the weakest link.
- Usability of security systems is a well-known concern
  - A. Whitten and J. Tygar. Usability of Security: A Case Study. Computer Science Technical Report CMU-CS-98-155, Carnegie Mellon University, 1998.
  - A. Whitten and J. Tygar. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *Proceedings of the 8th USENIX Security Symposium*, Washington, D.C., August 1999.
  - M. Zurko and R. Simon. User-Centered Security. In C. Meadows, editor, *Proc. of the 1996 New Security Paradigms Workshop*. ACM, 1996.
  - A. Kerckhoffs. La cryptographie militaire. *Journal des sciences militaires*, IX(38):5.38 (January) and 161.191 (February), 1883. Available at Fabien Petitcola's Website: <http://www.cl.cam.ac.uk/fapp2/kerckhoffs/>.

# MB: Risk Assessment

- Risk assessment is an integral part of security management
  - From a business perspective, security management is the process of implementing security controls for a ranked priority of risks that are deemed of significant impact.
- As already pointed out, it is recognized that usability is often the weakest link in the security chain of IT system.
- This implies that poor security usability actually represents a serious vulnerability in the risk assessment of systems.
- However, modern security and risk management standards do not seem to take security usability into account at all.
  - The term “*usability*” is not mentioned in “*ISO/IEC 27001:2006 Requirements for Information security management systems*” or in “*NIST Special Publication 800-30 – Risk Management Guide for Information Technology Systems*”
  - No references to usability on the National Vulnerability Database website.
  - Thus, it seems that poor security usability still does not appear on standard vulnerability checklists used by security analysts and experts.

# Implications of Current Landscape

- Security systems must be viewed as socio-technical systems that depend on the social context in which they are embedded to function correctly.
  - Security systems will only be able to provide the intended protection when people actually understand and are able to use them correctly.
- There is a very real difference between the degree by which systems can be considered theoretically secure (assuming they are correctly operated) and actually secure (acknowledging that often they will be operated incorrectly).
  - In many cases, there appears to be a trade-off between usability and theoretical security.
  - It may often be meaningful to reduce the level of theoretical security to improve the overall level of actual security.
- There is a need to outline how security usability can be included in standard risk assessment.

# Our Contribution

- A Taxonomy for Security Usability Approaches.
- A Set of Security Usability Principles.
- A Risk Assessment process that incorporates the Usability Principles.
- Sample Risk Assessments involving these Usability Principles.
- Guidelines for Security Usability Controls.

# Usable Security Approaches

- The trade-off between usability and theoretical security is not yet generally accepted as a fundamental principle in security design.
- We define two schools of thought, i.e. approaches:
  - *The Sustaining Approach*
    - Consider usability aspects from the beginning of the system development life cycle. No need to evaluate the underlying security building blocks, only how they are implemented.
  - *The Disruptive Approach*
    - Assumes security building blocks are inherently unsuitable for building user friendly security solutions. Replace them with other primitives that better support user-friendly security.

# Foundations of Security Usability

- Kerckhoff's security principles:
  1. The system must be substantially, if not mathematically, undecipherable;
  2. The system must not require secrecy and can be stolen by the enemy without causing trouble;
  3. It must be easy to communicate and remember the keys without requiring written notes, it must also be easy to change or modify the keys with different participants;
  4. The system ought to be compatible with telegraph communication;
  5. The system must be portable, and its use must not require more than one person;
  6. Finally, regarding the circumstances in which such a system is applied, it must be easy to use and must neither require stress of mind nor the knowledge of a long series of rules.
- Some of these principles are usability principles, which are still relevant, but overlooked over the last century.

# Principles of Security Usability Building Blocks

- The user's interaction points are the *security action* and the *security conclusion* stages.
- Formally:
  - A *security action* is when users are required to produce information and security tokens, or to trigger some security relevant mechanism.
    - For example, typing and submitting a password is a security action.
  - A *security conclusion* is when users observe and assess some security relevant evidence in order to derive the security state of systems.
    - For example, observing a closed padlock on a browser, and concluding that the communication is protected by TLS is a security conclusion.

# Principles of Security Usability

## Security Action Usability Principles

- A1. Users must understand which security actions are required of them.
- A2. Users must have sufficient knowledge and the ability to take the correct security action.
- A3. The mental and physical load of a security action must be tolerable.
- A4. The mental and physical load of making repeated security actions for any practical number of instances must be tolerable.

## Security Conclusion Usability Principles

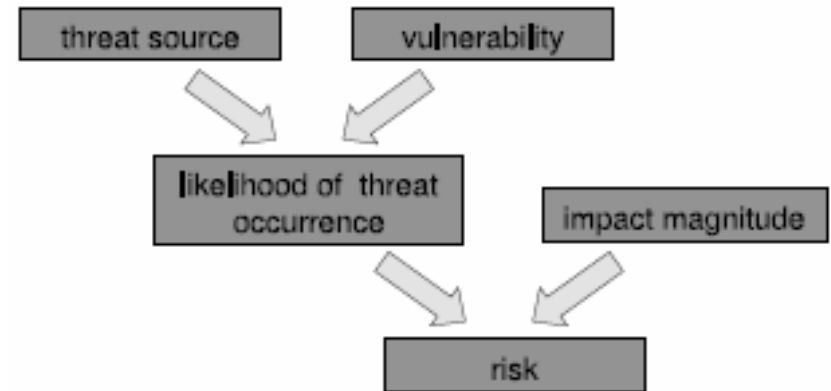
- C1. Users must understand the security conclusion that is required for making an informed decision.
- C2. The system must provide the user with sufficient information for deriving the security conclusion.
- C3. The mental load of deriving the security conclusion must be tolerable.
- C4. The mental load of deriving security conclusions for any practical number of instances must be tolerable.

*Derived from Kerckhoff's security principles #3 and #6.*

# Current State of Risk Assessment

## Definitions:

- A *threat source* can be an agent with malicious intent, an agent susceptible to non-intentional error, or a natural phenomenon.
- A *vulnerability* is a weakness that could be exercised or exploited to cause adverse events.
- A *threat* is a potential adverse event or action caused by a threat source that successfully exercises a particular vulnerability.
- Each threat has an associated *impact magnitude* which expresses the direct or indirect loss resulting from the threat occurrence.
- The *risk* of a threat is derived as the combination of the threat's likelihood and impact magnitude



Step 1.	System characterization
Step 2.	Threat identification
Step 3.	Vulnerability identification
Step 4.	Analysis of existing security controls
Step 5.	Likelihood determination
Step 6.	Impact analysis
Step 7.	Risk determination
Step 8.	Recommendation of new controls
Step 9.	Results documentation

# Usability and Risk Assessment

**PREMISE:** For threats, resulting from poor usability, to be captured, we need to explicitly consider poor security usability as a vulnerability. In order to do this, we need to update the relevant checklists used in Step 3 to include such vulnerabilities.

Security usability vulnerabilities on action	
SUV-A1	Users are unable to understand which security actions are required of them.
SUV-A2	Users do not have sufficient knowledge or are unable to take the correct security action.
SUV-A3	The mental and physical load of a security action is not tolerable.
SUV-A4	The mental and physical load of making repeated security actions for any practical number of instances is not tolerable.

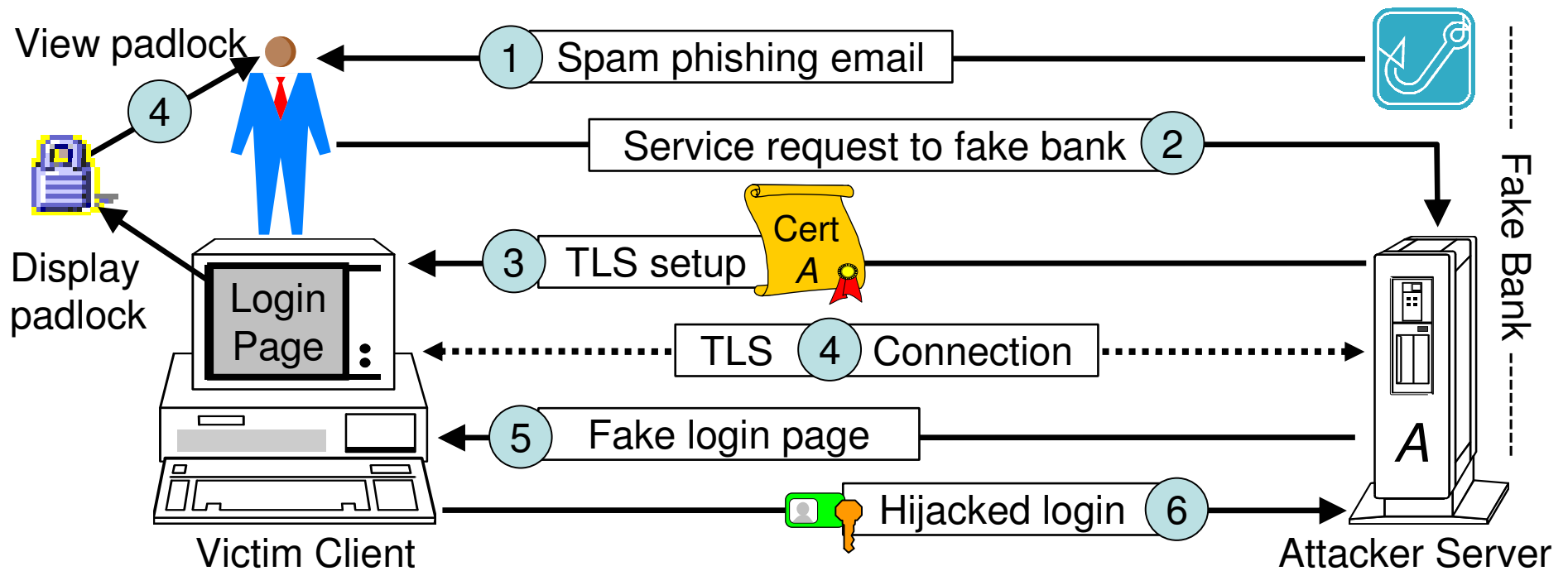
Security usability vulnerabilities on conclusion	
SUV-C1	Users do not understand the security conclusion that is required for making an informed decision.
SUV-C2	The system does not provide the user with sufficient information for deriving the security conclusion.
SUV-C3	The mental load of deriving the security conclusion is not tolerable.
SUV-C4	The mental load of deriving security conclusions for any practical number of instances is not tolerable.

We propose to define Security Usability Vulnerabilities as violations of the security usability principles previously presented. By adopting the abbreviation SUV to denote a Security Usability Vulnerability, each vulnerability can be referenced in a compact form.

# Case Study: Web Security Usability

- Current web security technology is based on the Transport Layer Security (TLS) protocol.
- It is normally assumed that TLS provides the *message confidentiality* and *server authentication* security services.
- This case study will demonstrate that the server authentication provided by TLS is mostly theoretical, and meaningless in practice due to poor usability.
  - This will be done by comparing the security solution with the security usability principles previously described above, it can easily be seen why the security fails in this case.
- Though based on strong cryptography, there are a number of security exploits that TLS cannot prevent, e.g. phishing, which is a combination of social engineering and man-in-the-middle attacks.

# Phishing Attack

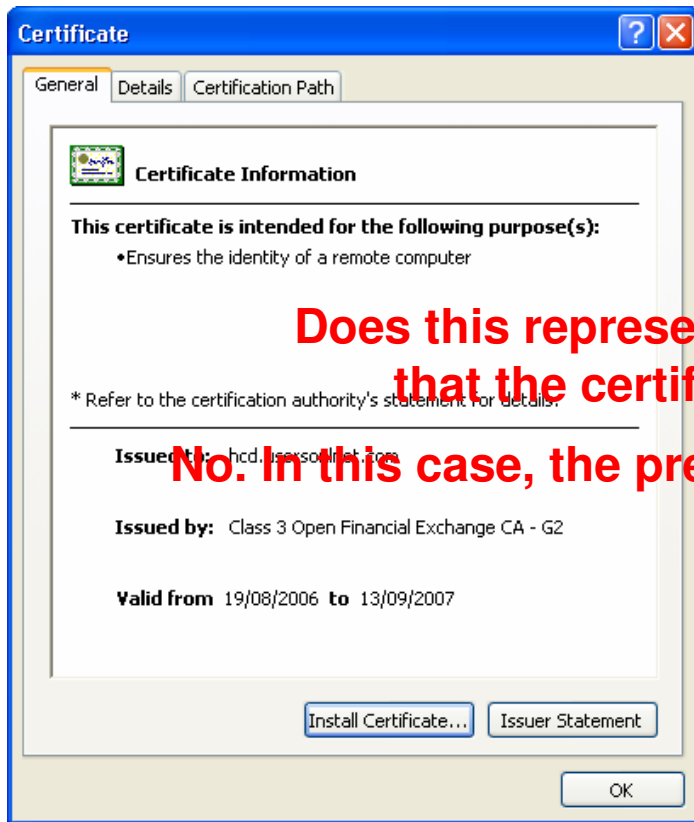


- **Technically** – The Fake Bank has been correctly authenticated using TLS
- **Semantically** – This is a False Positive, i.e. the client has wrongfully authenticated the server.
- **Problem:** None of the information provided is sufficient to make an informed decision about the identity of the web server.

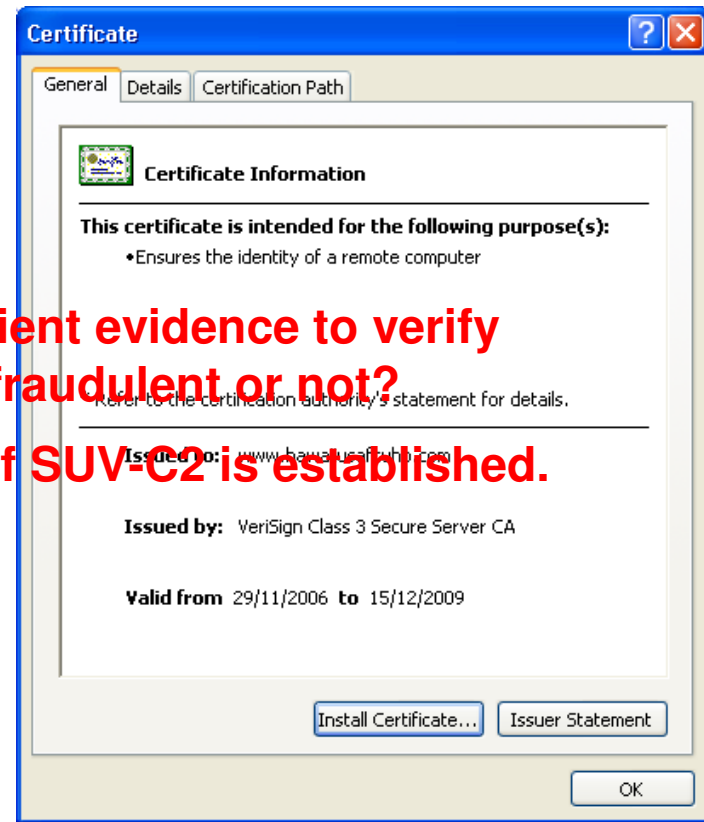
# TLS Usability Cues

- The closed padlock
  - Indicates that web session is protected with TLS
  - Simple to interpret and causes negligible mental load
  - However, it says nothing about the server's identity, which implies SUV-C2
  
- The server's certificate
  - Can be obtained by double-clicking on the padlock
  - The mental load of analyzing the content of a server certificate is at least intolerable, which implies SUV-C3 and SUV-C4
  - SUV-C2 could have been eliminated had the certificate provided sufficient information to derive the correct security conclusion, but it seems like this is not the case in the majority of scenarios.
    - Let's examine a real case, that demonstrates that absence of SUV-C2 is more likely to be the general case, rather than the exception.

# Hawaii Federal Credit Union Attack (March 2007)



Certificate for  
www.hawaiiifcu.com



Certificate for  
www.hawaiiusafcuhb.com

**Does this represent sufficient evidence to verify  
that the certificate is fraudulent or not?  
No. In this case, the presence of SUV-C2 is established.**

# General Insight

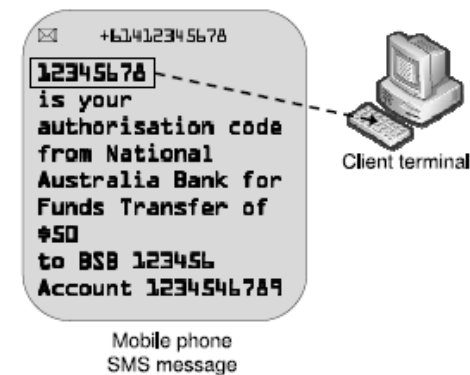
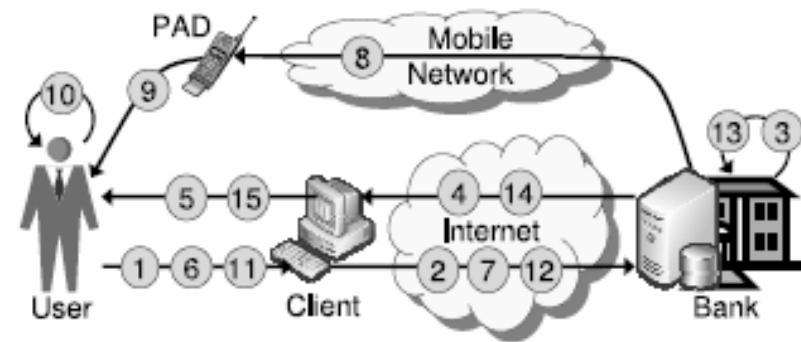
- The certificate's issuance policy, stated in the "*issuer statement*", may provide sufficient information to judge the legal status of a certificate.
  - However the size of this document (a 2,666 Word document, approx. 4 full standard pages) indicates the presence of vulnerability SUV-C3, as well as SUV-C4.
- Peer-Entity Authentication is "the corroboration that a peer entity in an association is as claimed".
  - In phishing attacks, the attacker claims its own identity (in the formalism of TLS), and the TLS client simply verifies the correctness of that claim.
  - However, the claimed identity expressed in the certificate does not correspond to the identity that the user assumes. Thus, the problem is one of **identity representation** and **identity mapping**.
- Generally, vulnerabilities SUV-C1, SUV-C2, SUV-C3 and SUV-C4 are present in web security scenarios.

# Transaction Authorization Usability

- In reaction to the stream of phishing attacks, many banks have rolled out additional security solutions.
  - Some banks issue special hardware tokens that can generate one-time authorization codes,
  - Other banks rely on out-of-band communication to the customer's communication device of choice.
- In the latter approach, transactions can be authorized using SMS messages sent to the user's mobile phone.
  - Although the user has been authenticated and is already logged in, this allows authentication of the transaction request itself.

# Transaction Authorization with SMS

- SMS messages sent from the bank to the user's mobile phone via the cellular network, which is assumed to be independent of the Internet.
- The user transfers data from the mobile phone to the client terminal.
- By verifying the correct transfer of data, the bank can conclude that the user received the data through the cellular network, read it and submitted it through the Internet.
- This is interpreted as a genuine intent to submit the transaction.



# Security – SMS Transaction Authorization

- Assuming that the user can verify the correctness of the amount and of the bank account number in SMS consistently and reliably, this is secure against attacks on the client terminal.
- This scheme assumes that the mobile terminal can be trusted.
- This scheme also depends on the security of the mobile phone networks, and it assumes that no attacker is able to modify SMS messages sent to the user while in transit through the mobile network.
  - Even if interception and cryptanalysis of the SMS messages sent over the air were possible, it requires that the attacker is physically present in the same base station coverage area, which excludes attacks from many places in the world.

# Risk Assessment of SMS Transaction Authorization

- Attack Scenario:
  - An attacker changes the amount and or the destination account number, e.g. by a Trojan program on the client terminal, and the modified amount and account number appear in the SMS message.
- How do we know this is likely?
  - In a study of the usability of SMS authorization, it was found that 21% of participants failed to notice when the destination account number was modified under a simulated attack\*.
  - Thus, in 1 of 5 attacks the assumption that the correctness of the amount and of the destination account number is verified by the user when copying the authorization code from the SMS message is false.
- Consequence:
  - Despite being the victim of an attack, the liability could be put on the user because he accepted the SMS message. This indicates the presence of vulnerability SUV-C4.

\* M. AlZomai, et. al.. An Experimental Investigation of the Usability of Transaction Authorization in Online Bank Security Systems. In *The Proceedings of the Australasian Information Security Conference (AISC2008) (to appear)*, Wollongon, Australia, January 2008.

# The Analysis

- We conducted a simple usability risk assessment of the out-of-band SMS authorization method.
- The identified vulnerability SUV-C4 can be combined with relevant threats to form a set of vulnerability-threat combinations.
- The vulnerability and threat source that we considered are:
  - **Vulnerability SUV-C4:** Users failing to notice that the destination account has been changed. Then making the wrong conclusion that the transaction integrity is preserved.
  - **Threat Source:** Hackers and computer criminals attempting to conduct fraudulent bank transactions.
  - **Threats:** T1. **Smart Trojan Threat;** T2. **Pharming and Man-in-the-Middle Threat**
- While the smart Trojan threat and the man-in-the-middle threats require advanced technical skills to be executed, we consider their likelihood to be “*Possible*” in terms of the risk matrix (pg 271 of proceedings).
- Assuming that attackers are able to conduct fraudulent transactions, considerable amounts of money can be diverted. Thus, we consider the impact magnitude to be “*Major*” in terms of the same risk matrix.
- The likelihood and impact together indicate that this poses a “*High Risk*”.
- We predict that it is only a question of time before this risk will materialize on a wide-scale.

# Conclusion

- We have described a set of security usability principles.
- We have shown how these principles can be used to define vulnerabilities for conducting risk assessments.
- We have demonstrated that it is necessary to integrate the assessment of security usability in the risk assessment and security management of systems in order to properly manage current and emerging risks.
- We have highlighted that it can be challenging to find and or build appropriate security controls for mitigating poor security usability.
- We have pointed out that suitable controls can be identified either through a sustaining approach or a disruptive approach.
- We provided guidelines for constructing these security usability controls.



**More Information:** <http://www.almaden.ibm.com/software/disciplines/iis/>

**Contact:** Dr Audun Josang (a.josang@qut.edu.au)

Dr Tyrone Grandison (tyroneg@us.ibm.com)