Visual Mutual Authentication
An Approach to
Secure Online Banking

hgi
Horst-Görtz Institut
für IT Sicherheit

Authentification as a User - Challenge

Authenticate a server to a user: Certificates

Problem: How to verify a certificate?

Threats: Phishing, Pharming, MITM, PKI-Problems

Authenticate a user to a server: Submit challenge (password)

Problem: Is the user's PC trustworthy?

Threats: Malware, Remote Desktoping Attacks

Conclusion: Path between user and server is considered to be untrustworthy

Idea: Authentication with non-computational components

Solution: Visual Cryptography [1]

Visual Cryptography – The basic principle

Elements of Visual Cryptography for authentication:

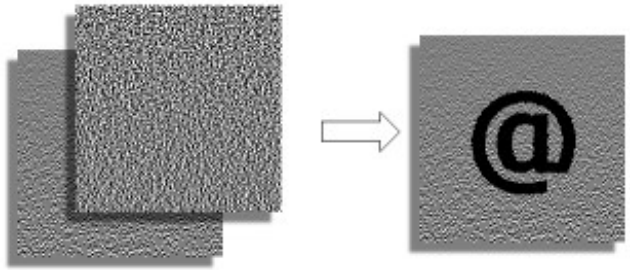
1. Generate user key (by random)

2. Decryption:

Share a white pixel

Share a black pixel

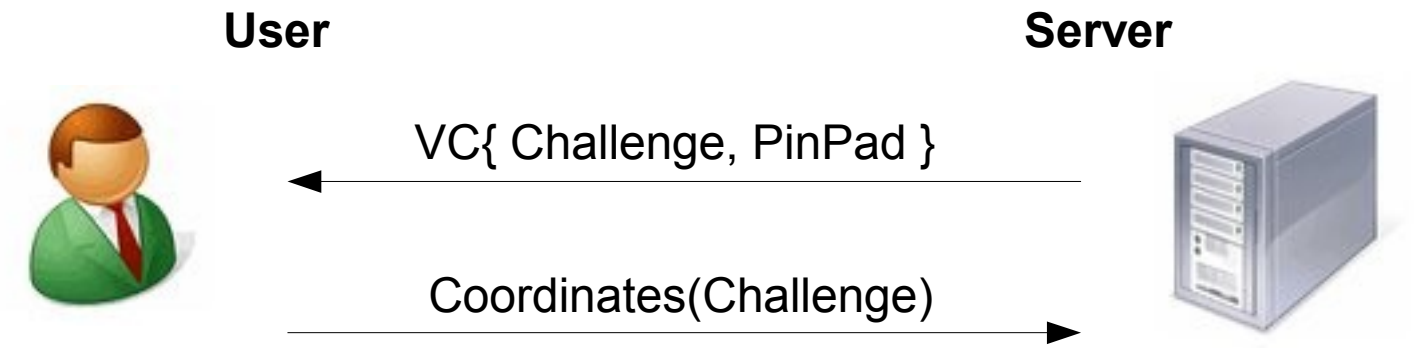
3. Encryption:



Two out of two shared secred scheme with one-time pad characteristic

VMA – Visual Mutual Authentication

Visual Cryptography to establish a secure channel between a user and a server:



VMA – Application to Online Banking

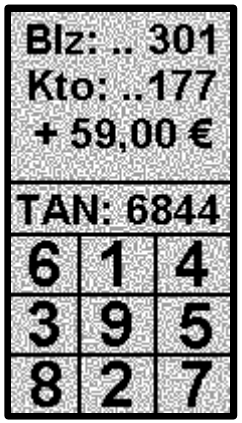
User

Server

Transaction - Data

VC{TAN, PinPad, Data}

Coordinates



VMA – Advantages

- Secure channel without an underlying trustworthy system
- Efficient: no computation and no special software or hardware on the user's PC necessary
- Theoretical perfect security (One-Time Pad)
- Very easy for the user to understand and to deploy

Current State – Future work

Current state:

Java Applet implemented

Future work:

- Usability and deployability study
- Tolerance in application of the transparencies
- Increased entropy (other alphabets, hash-functions, colored VC)

VMA – An Approach to Secure Online Banking

Thank you for your attention!

Horst-Görtz Institut für IT Sicherheit

References

[1] Naor M. and Shamir A., *Visual Cryptography*, Eurocrypt '94, Springer-Verlag LNCS Vol. 950, Springer-Verlag, 1995, 1-12.