Concepts against Man-in-the-browser Attacks

Philipp Gühring

web manuscript, published circa January 2007.
Available: http://www2.futureware.at/svn/sourcerer/CAcert/SecureClient.pdf
13, October, 2008.

Summary

- The problem: Points of attack; methods of attack.
- The risk assessment: In 2008,some opinions already out of date.
- Solution concepts:
  - ✓ Secure client
  - ✓ Second Channel
  - ✓ Secure communication.

Appreciation

- Precisely stated

The problem:

"No advanced authentication method can defend against [Man-in-the-browser]these attacks"

Solution concepts:

- Multi-path passwords
- Shared Secrets
- External authorisation devices

Online recourses(examples): works on authentication level, contradict with his statement before.

"Authentication systems that use the PC as the single channel for transaction data to the server are circumvented."

Appreciation

- Clearly demonstrates MITB's threats

Method of Attack

"1. The Trojan infects the computer's software, either OS or application."

……(2-17)

"18. The user thinks that the original transaction was received by the server intact and authorized correctly"

- ✓ Online transaction: People daily use.
- ✓ Step by step: From infect to make a attack

Criticism

- No strong evidence support his opinion

  For Example:

  "It is known that FireFox, Internet Explorer and Opera are successfully targeted"

  I would doubt about this, and I think Microsoft also would argue about this.

  "[Using Virtual Machine] raises the cost of the attack."

  Why I can't think It make the attack easier because if I infect the host system, I can also infect all the virtual systems running on this host

Question?

- Except solution concepts mentioned in this paper, Do you have other solutions ?

Hints:

Recall Lampson's Computer security in the real world.

Five defensive strategies:

Isolate ; Exclude; Restrict; Recover; Punish

Author's concepts only focus on one or two strategies of this five

Why not others ?