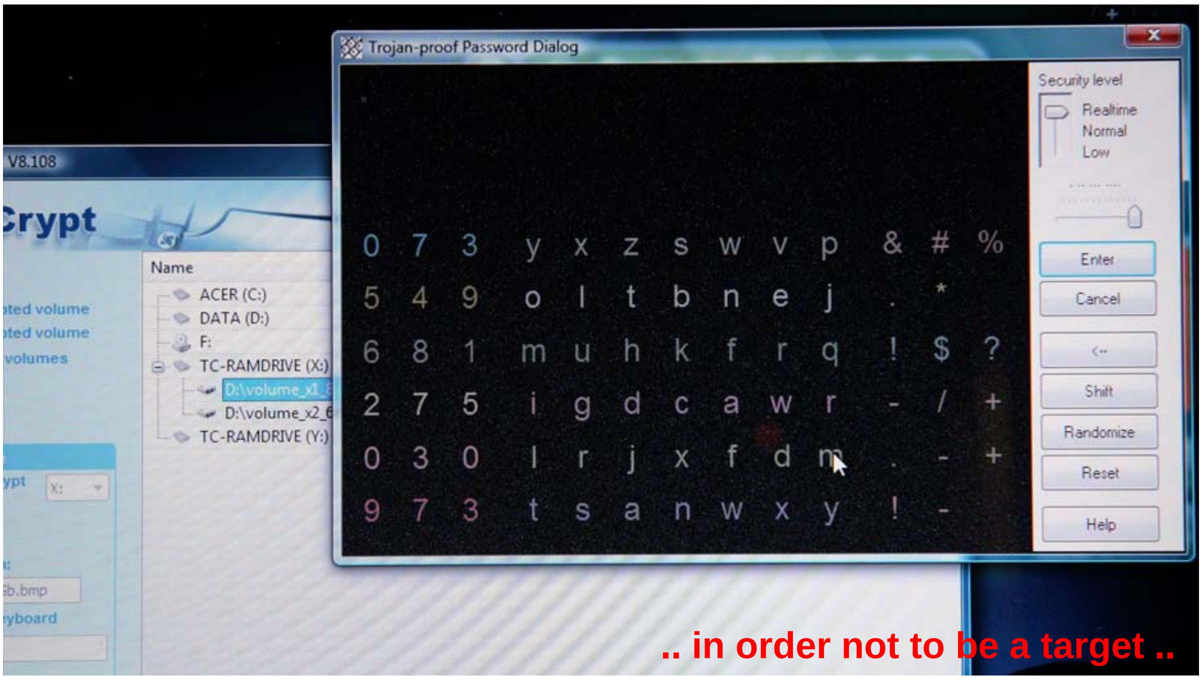


.. in order not to be a target ..

The Trojan-Horse-Proof Virtual Keyboard

First published: July 2008

The Trojan-Horse-Proof Virtual Keyboard

White Paper

For the latest information, please see http://www.pmc-ciphers.com

Introduction

Professional hackers and assigned organisations like intelligence agencies are recently developing a number of trojan-horses that can potentially target anybody.

Very evident is the way how data is collected and what kind of data is of interest:

Passwords – collected via Internet

Why passwords? They are short but powerful as they give access to:

- e-mail accounts
- bank accounts
- ordering systems and internet communities
- encrypted data (encryption is generally used by people who have something to hide: like music, love letters, pictures of naked women or other personal and thus “highly suspicious” data)

Passwords further seem to be easily accessible.

How is password data collected?
By intercepting information sent from your keyboard to your computer. Keystrokes can either be recorded by a hidden piece of hardware in the keyboard or they are simply logged by malicious software – so called “Trojan Horses”. While normal criminals sometimes use the first approach do professional hackers and assigned organisations generally prefer the latter approach.

What is a Trojan Horse?

The term is defined as a program that looks like having a useful and desired function. The software performs undesired functions – at least sometimes. The seemingly useful functions are nothing but camouflage for the functions that are undesired for the user. A Trojan Horse always does malicious things that are unknown to the user.
Real-world Trojan Horses usually contain spying functions or backdoors that allow to control the computer from a remote location.

Today the term is mixed with computer viruses, simply because there exist computer viruses that report gathered information “home” to a server which belongs to the hacker who has created the Trojan Horse. In the classic sense although were Trojan Horses not designed to spread themselves. Trojan Horses can be polymorphic (encrypted with different passwords with an identical crypto engine) and they can even run in the system context of the operating system!
The latter is actually the biggest threat. A Trojan Horse that has not been designed to spread itself can look like any useful piece of software – applications, self-registering DLLs and software drivers. Kernel-mode software drivers are generally created in the system context of the operating system. Such

software has access to all kinds of user data.

Short summary: Hackers prefer to target passwords and they use Trojan Horses to gather this data.

What if a clever piece of software would enable users to enter passwords so that no Trojan Horse could ever log such data?

Would be pretty neat !

The Trojan-Horse-Proof Virtual Keyboard

The photo below shows our invention of a virtual keyboard that allows for totally secure password entry. Conventional OTFE (On-The-Fly-Encryption) software - or encryption software in general - only allow for password entry by keyboard (or by smart cards and other authentication methods that are not suitable for guaranteeing perfect secrecy).

Well, it's flickering and somewhat exhausting to use, but this thing is one of the most decisive inventions in computer security – at least when it comes down to trying to keep a little bit of privacy.

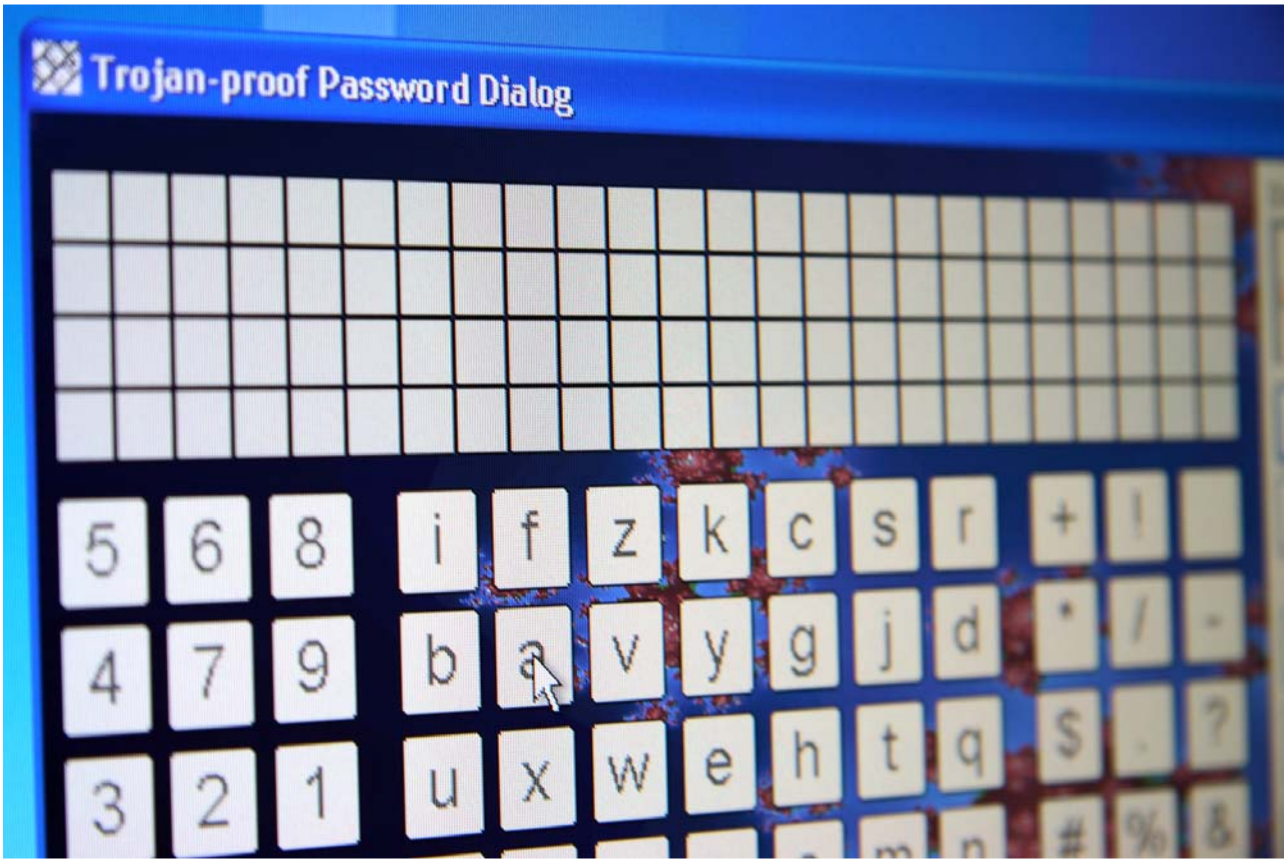
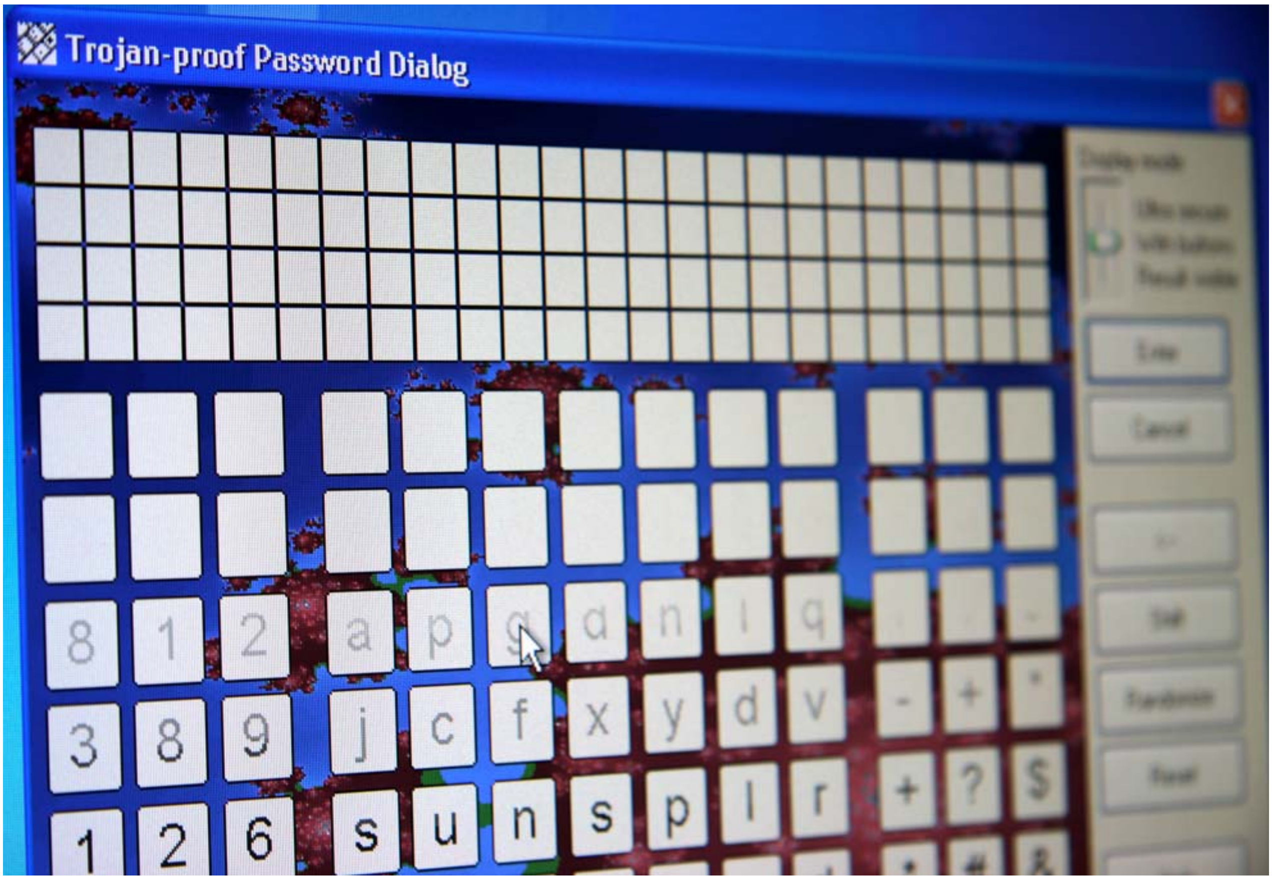

Trojan-proof Password Dialog
5 6 8 i f z k c s r + !
4 7 9 b a v y g j d * / -
3 2 1 u x w e h t q $. ?
m n # % &

Fig. 1 Trojan-Horse-Proof password dialog implemented in TurboCrypt OTFE (disk encryption) software

Features:

- No Trojan Horse can spy on passwords that are entered in this Trojan-Horse-Proof Virtual Keyboard.
- Runs theoretically on any multitasking operating system.
- Is built into the disk encryption software “TurboCrypt” from Global IP Telecommunications / PMC Ciphers.
- Can be tested for free by downloading TurboCrypt here: http://www.turbocrypt.com .
- Video cameras are the only potential risk. Please make sure that no camera can make screenshots while you’re entering your passwords.
- Costs no money at all as no special hardware is required.
- Is the only available solution to prevent trojan horses from gathering passwords!
- Is a little tedious to use. Users who prefer to have no secrets at all are asked to forward all their data to the next best hacker in the neighbourhood.

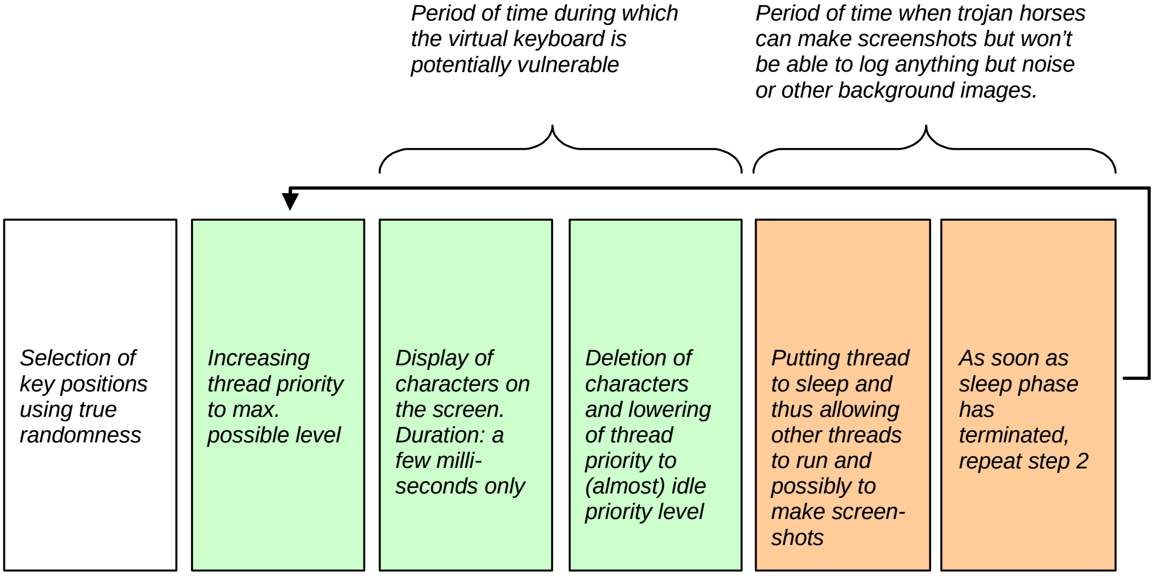
How does the Trojan-Horse-proof Virtual Keyboard work?


Trojan-proof Password Dialog
8 1 2 a p g d n l q
3 8 9 j c f x y d v - + *
1 2 6 s u n s p l r + ? $

In any case does our invention provide perfect secrecy for your passwords as the trojan-horse-proof virtual keyboard does not allow any malicious piece of software to gather any useful information.

The photo actually reveals the mode of operation of the virtual keyboard. Key characters are painted, deleted, painted again and deleted again. This sequence repeats itself several times per second. In order to keep highly intelligent trojan horses from taking a snapshot of the screen while all characters are visible, a characteristic that is inherent to the task scheduler, which is implemented in the core of the operating system, is exploited:
Processes running at realtime priority level will probably never be descheduled by processes featuring a lower priority level. Even processes with the same (very high) priority level won’t interrupt our virtual keyboard process as long as the virtual keyboard does not consume too much CPU time. It wouldn’t make must sense for the scheduler to interrupt a media player application by a process that e.g. indexes e-mails in the background. The operating system wouldn’t be popular if audio or video playback was choppy.

This is the sequence of operations executed by the Trojan-Horse-proof Virtual Keyboard:


Period of time during which the virtual keyboard is potentially vulnerable
Period of time when trojan horses can make screenshots but won't be able to log anything but noise or other background images.
Selection of key positions using true randomness
Increasing thread priority to max. possible level
Display of characters on the screen. Duration: a few milli-seconds only
Deletion of characters and lowering of thread priority to (almost) idle priority level
Putting thread to sleep and thus allowing other threads to run and possibly to make screen-shots
As soon as sleep phase has terminated, repeat step 2

It should be noted that modern microprocessors feature at least two independent CPU cores. TurboCrypt uses up all available CPU time on all but one CPU core to compute pseudorandom numbers in order not to give any malicious piece of software any access to CPU time.

This fascinatingly simple but highly efficient method keeps hackers away from your password data. The tool has been thoroughly tested by us for many months. You can test the efficiency easily by yourself with the help of a frame grabber tool or our Screen DC grabber, a test tool that takes screenshots at realtime priority level and that displays these screenshots instantly. If this tool rarely displays key characters of the virtual keyboard, you can be sure that your timing settings are good and that no Trojan Horse can gather any screen information successfully. It is further suggested to test the efficiency of the algorithm with screen grabber tools like Camtasia or CapturePad.

Even if a number of Trojan Horses (i.e. malicious computer software or possibly a computer virus which report all keystrokes and/or screen content back to the server of a criminal or an assigned organisation) have infected the user's computer, users can still be sure that their password remains completely secret.

For more information: http://www.pmc-ciphers.com

This is a preliminary document and may be changed substantially prior to final commercial release. This document is provided for informational purposes only and PMC Ciphers & Global IP Telecommunications make no warranties, either express or implied, in this document. Information in this document is subject to change without notice. The entire risk of the use or the results of the use of this document remains with the user. The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of PMC Ciphers or Global IP Telecommunications.

PMC Ciphers or Global IP Telecommunications may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from PMC Ciphers or Global IP Telecommunications, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.