Valery Konyavsky

VNIIPVTI
All-Russia Research-and-Development Institute for Problems of Computing Equipment and Informatization
001@pvti.ru

New Approaches to Ensure Cybersecurity

Sofia, 2008

A personal computer

is only an instrument.

Are you sure that
YOUR PC

is only YOUR
instrument?

Are you sure about it

EACH TIME

that you turn it on?

You need the assurance

that while you were away

- ✓ no PC hardware has been changed;
- ✓ no PC software has been changed;
- ✓ no data, stored on your PC, has been changed

or became known to an intruder.

In order to provide security,

and not simply protect,

it is necessary to understand
what exactly is the

OBJECT OF PROTECTION.

The objects of information protection

are defined by the things that the intruder's activities may be aimed at:

- ✓ the computer equipment (CE);
- ✓ the data that is stored and processed by the CE;
- ✓ data processing technologies;
- ✓ data transmission channels.

The goals of the information protection

are defined in accordance with the objects:

- ✓ protecting your computer from the unauthorized access;
- ✓ delimitating the data access rights;
- ✓ providing the invariability of the data processing technology;
- ✓ transferring data in a protected form.

The goals of the information protection

are solved **by using the unauthorized access control product**

Accord-TSHM

and the information protection systems, which are based on it.

The first task of information protection is

protecting your PC from an unauthorized access (UA).

An UA protection tool must:

✓ allow working on this PC only for those users who have a right to work on this PC, according to the security policy;

✓ control the state of the computer hardware and software for the absence of any unauthorized modifications.

What should an UA protection tool be like?

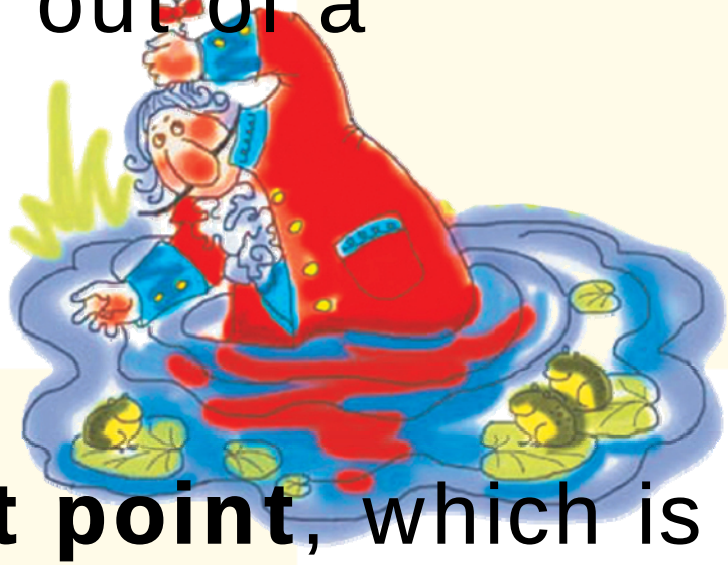
Checking the integrity of the **software environment** with the help of some **program** — can we be sure in its own integrity?

First, we need to **check that program.**

And before that — **check the program** that is going to check it...

What should an UA protection tool be like?

Can you pull **yourself** out of a swamp?



You can.

If you have a **support point**, which is **outside of the swamp**.

What should an UA protection tool be like?

- ✓ **independent** from the PC operating and file system
- ✓ **inaccessible** for the introduction of modifications
- ✓ **hardware-based.**

At the end of last century, we have developed a concept of hardware protection and an Data Security Tool (DST),

which became and still **remains a standard** for all of the developers.

Accord-TSHM:

Trusted Startup Hardware Module

Provides a **secure boot** of the operating system, irrespective of its type, for an authenticated user.

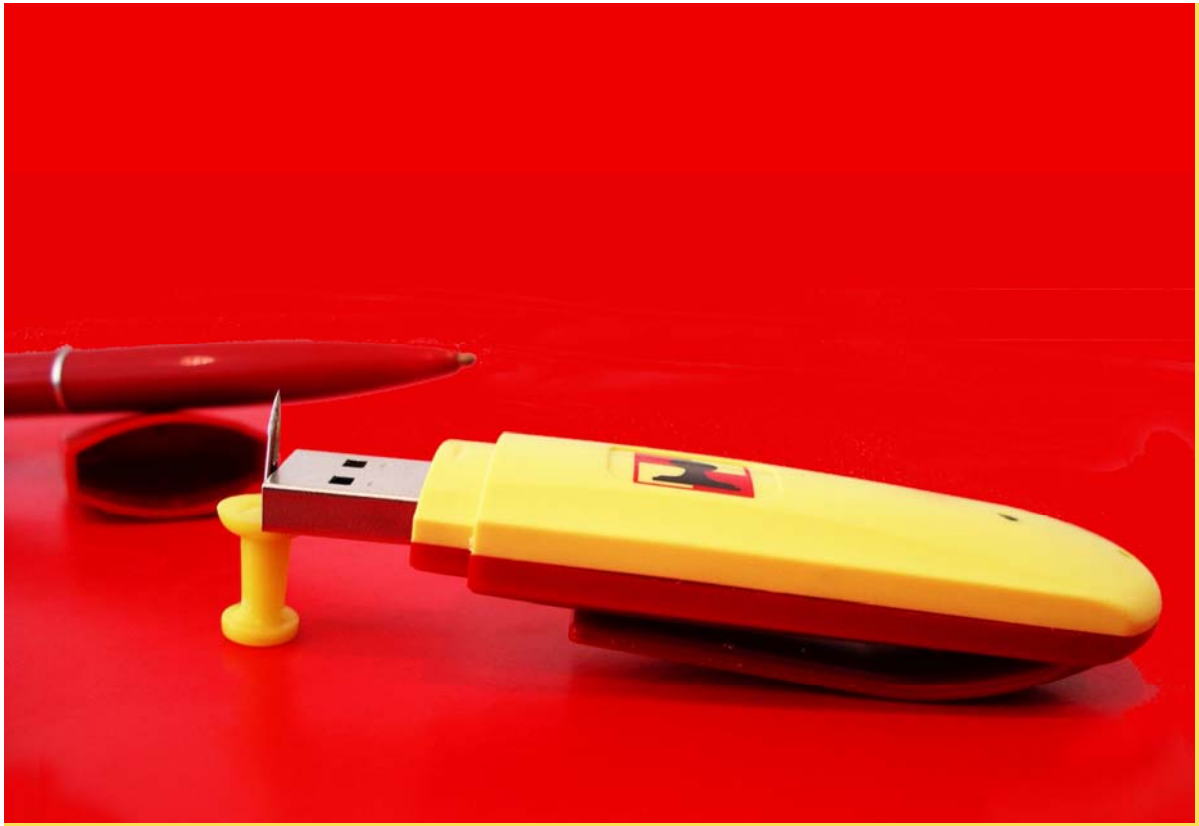
What is secure boot?

The operating system boot is performed only **after** a successful completion of the following procedures:

- ✓ the user identification/authentication.
- ✓ integrity checking of the PC hardware and the software utilities, using a step-by-step integrity inspection algorithm;
- ✓ blocking the operating system boot from the external storage mediums;

Accord-TSHM:

- ✓ has been patented
- ✓ has **28** **conformance certificates**
- ✓ and has more than **250 000** implementations in the governmental authorities and commercial organizations, as of the end of the year 2008.



PERSONAL cryptographic data security tool (PCDST)

SHIPKA

Ideal information interoperability:

- Mobile
- User-friendly

and

- Protected

Real life confronts you with an alternative:

- Mobile
- User-friendly

OR

- Protected

Real life confronts you with an alternative:

Using confidential information

- Mobile
- User-friendly

OR

- Protected

Real life confronts you with an alternative:

Storing the passwords for the web-services and the encryption keys/ Electronic Digital Signature (EDS)

- **Mobile**
- **User-friendly**

OR

- **Protected**

Real life confronts you with an alternative:

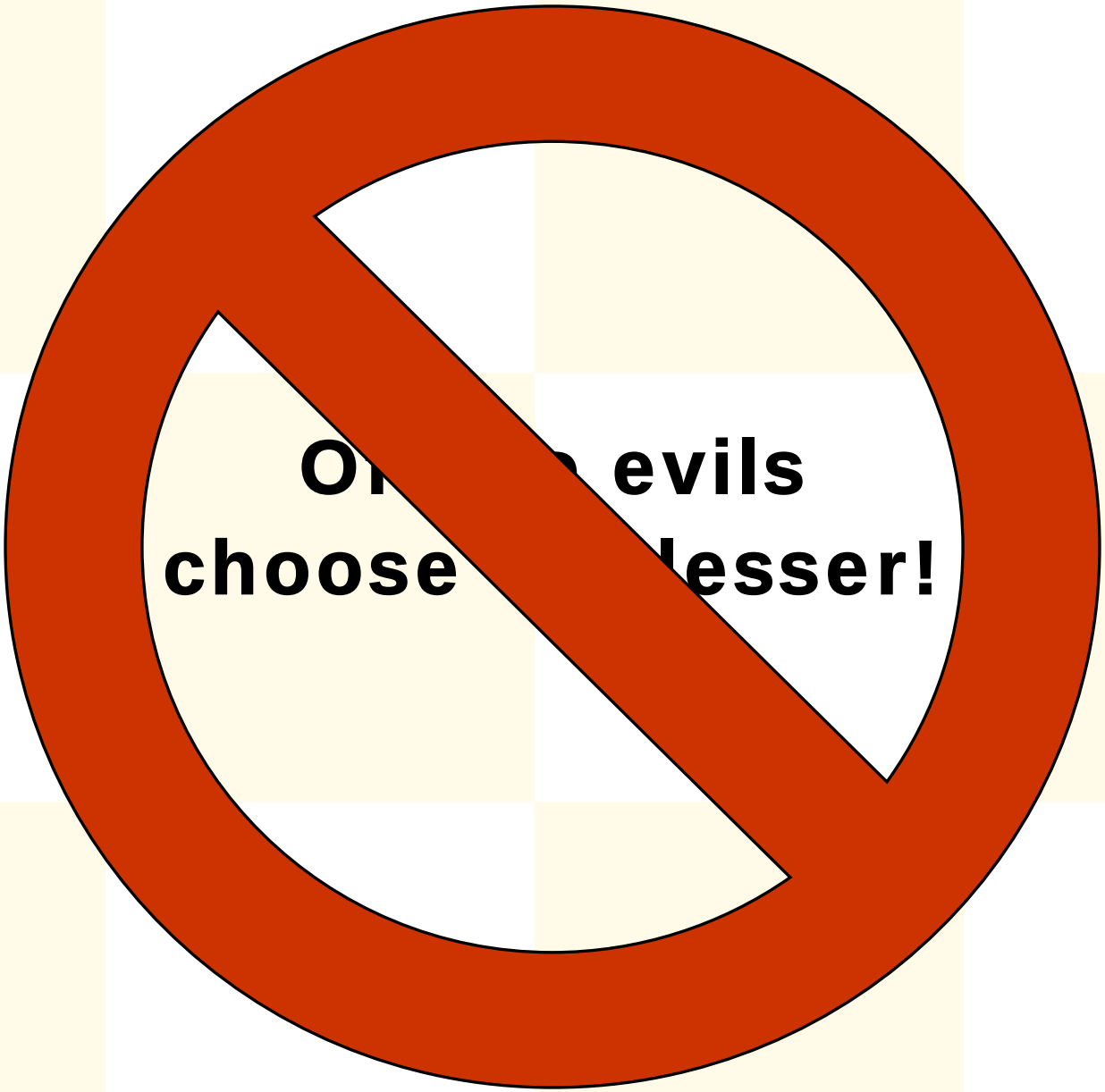
Banking account administration

- Mobile
- User-friendly

OR

- Protected

Of two evils
choose the lesser!


evils
choose lesser!

In order to have everything you need, it's enough to have PCDST SHIPKA with you.

PCDST SHIPKA

✓ **Mobility:** doesn't require software installation from additional carriers; may be used at any PC, which has an USB-plug.

✓ **User-friendliness:** doesn't require cryptographic libraries installation on PC; provides safe storage and application of the personal confidential data; doesn't require any special skills when operating on PC or in the Internet.

✓ **Protectability:** hardware implementation of the cryptographic algorithms, protected random number generator, protected permanent memory, applying the keys without transferring them to PC.

Main solutions, using SHIPKA

We offer to use PCDST SHIPKA:

- ✓ for the **encryption and/or signing of the files;**

Main solutions, using SHIPKA

We offer to use PCDST SHIPKA:

- ✓ for the **automatic filling of the WEB-forms** of various WEB-services and for **storing passwords** and other data, required for that;

Main solutions, using SHIPKA

We offer to use PCDST SHIPKA:

- ✓ for the **hardware identification and authentication** on PCs and notebooks when booting OS Windows, as well as in the terminal solutions;

Main solutions, using SHIPKA

We offer to use PCDST SHIPKA:

- ✓ as a **keys storage and a hardware-based random number monitor** for the cryptographic applications;

Main solutions, using SHIPKA

We offer to use PCDST SHIPKA:

- ✓ as a **“smart-card”** in the template solutions, for example, the authorization when entering the Windows domain, encryption and/or signing of the messages in the mail programs (Outlook Express and so on), for obtaining the Verification Center certificates;

Main solutions, using SHIPKA

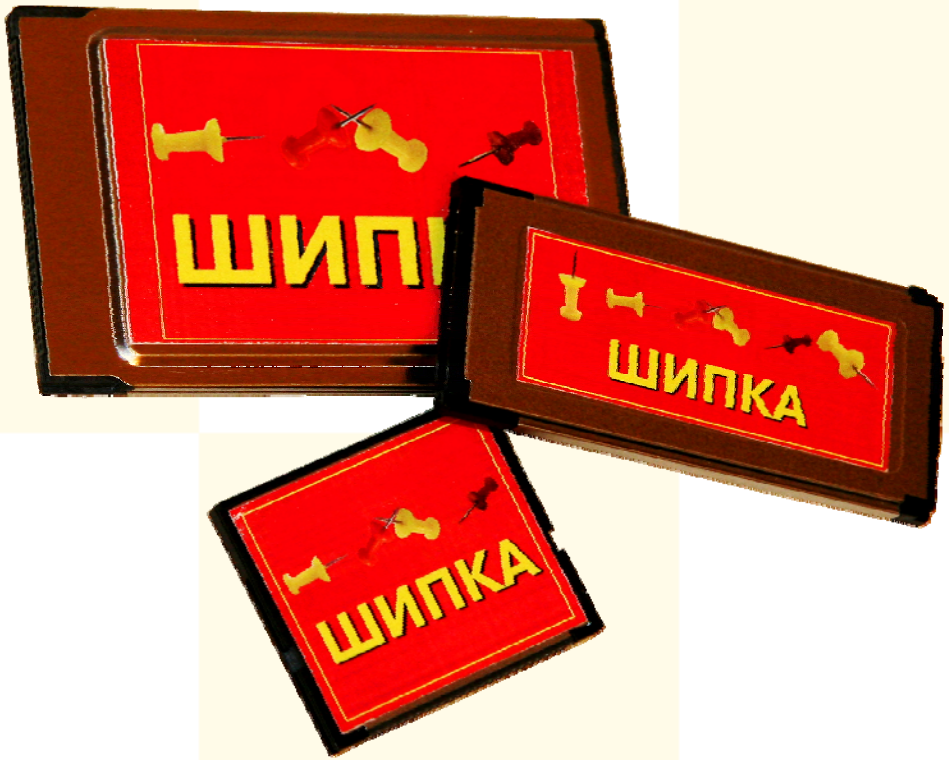
We offer to use PCDST SHIPKA:

- ✓ for the **informational technologies protection** with the help of the Authentication Protection Code.

Today PCDST SHIPKA is not only USB-device

But also

- ✓ PCCARD
- ✓ ExpressCard
- ✓ Compact Flash



Carry everything you need with you!

Valery Konyavsky

VNIIPVTI
All-Russia Research-and-Development Institute for Problems of Computing Equipment and Informatization
001@pvti.ru

Please, ask your questions!

New Approaches to Ensure Cybersecurity

Sofia, 2008