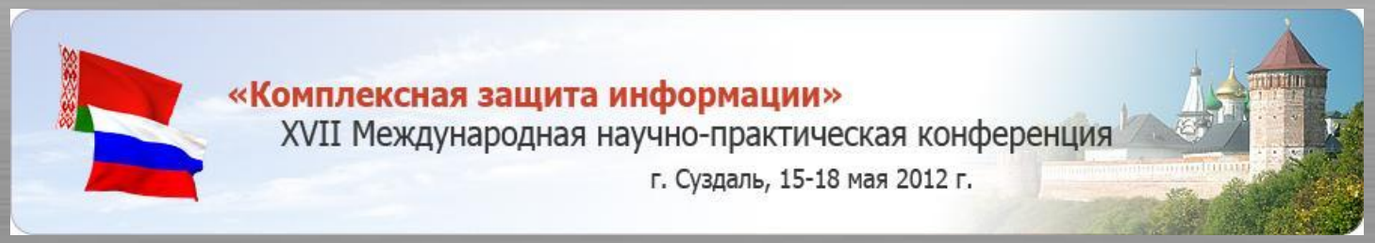


КЛАССИФИКАЦИЯ АППАРАТНЫХ ЗАКЛАДОК И МЕТОДОВ ЗАЩИТЫ ДЛЯ РЕШЕНИЯ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Барановский Олег Константинович
Государственное предприятие «НИИ ТЗИ»
Минск, Республика Беларусь

Угрозы применения закладных устройств в СВТ

- Утечка информации
- Повреждение (изменение, уничтожение) информации
- Нарушение штатного режима (прекращение) функционирования СВТ

Зараженность АСУ ТП вирусом Stuxnet

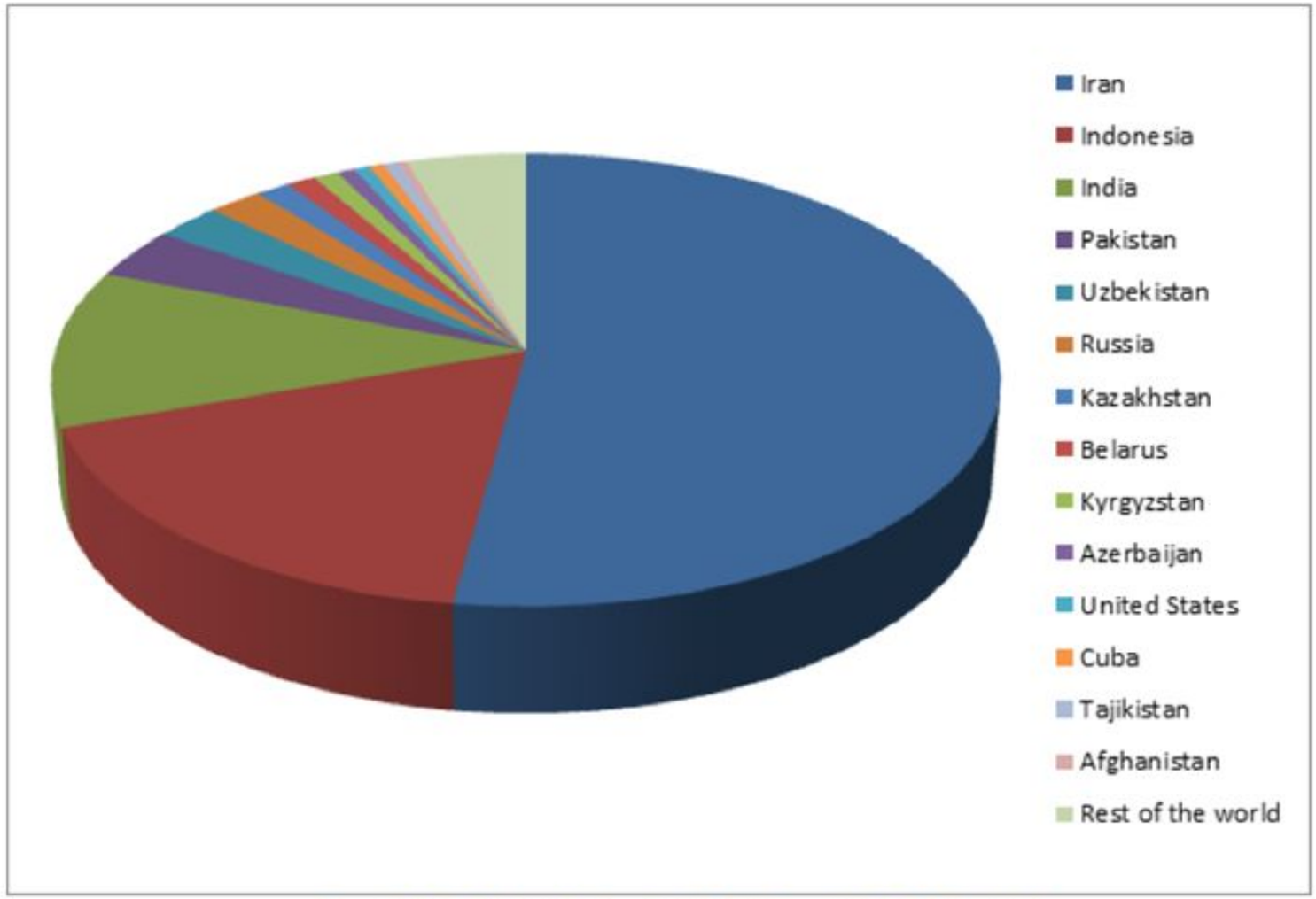


Figure 1.4.1 – Global infection by Win32/Stuxnet (Top 14 Countries)

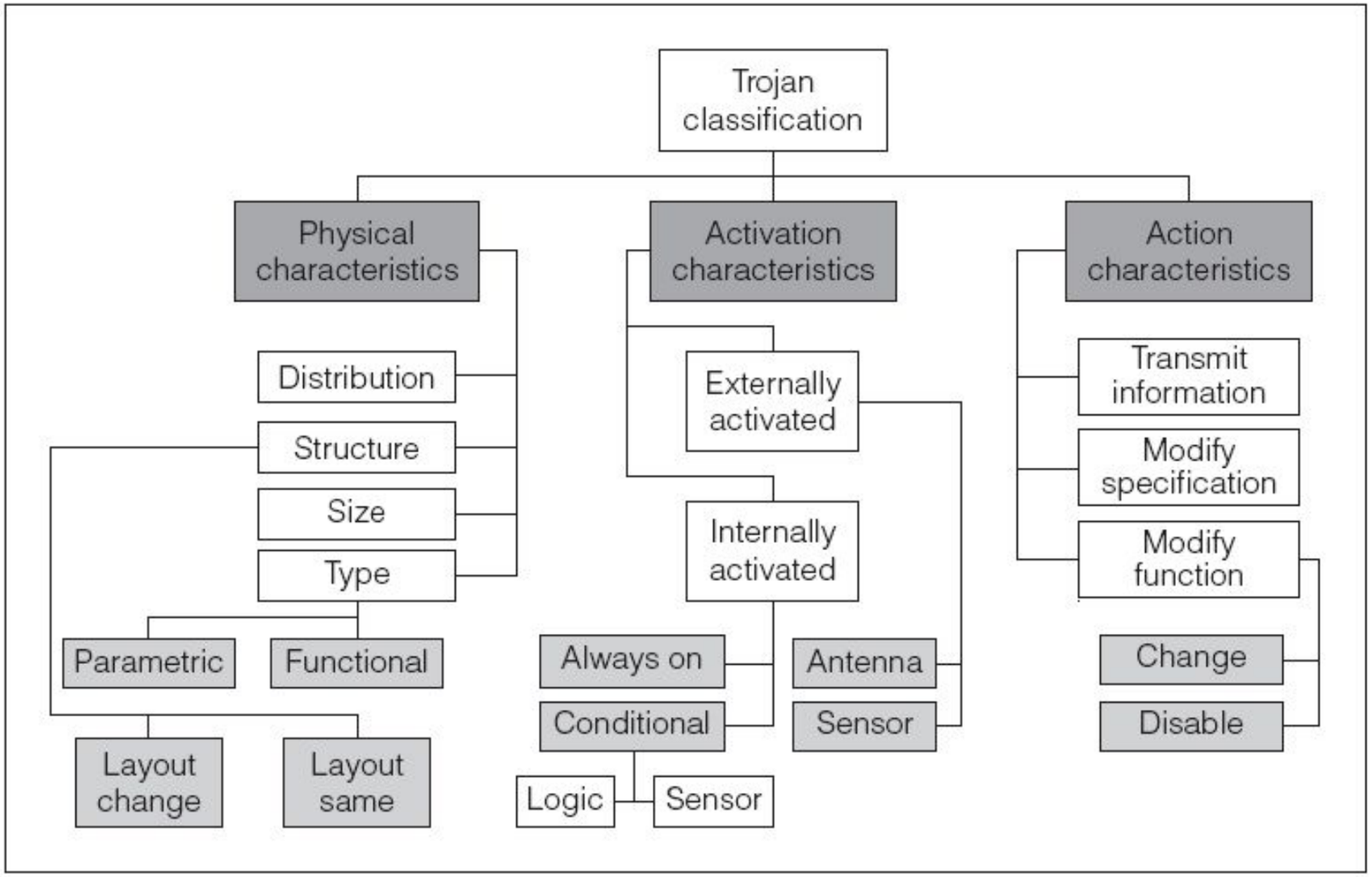
Классификация ЗУ перехвата информации, внедряемых в СВТ

Вид перехватываемой информации	1. Видеоизображение, выводимое на экран монитора. 2. Информация, вводимая с клавиатуры. 3. Информация, выводимая на принтер. 4. Информация, записываемая на жесткий диск компьютера (HDD). 5. Информация, записываемая на внешние накопители (flash-память, CD, DVD, USB-накопители). 6. Информация, передаваемая по каналу связи.
Место установки	1. В корпусе системного блока. 2. Подключаемые к внешним разъемам системного блока (например, USB). 3. Подключаемые в виде переходных элементов в разрыв информационных кабелей, соединяющих системный блок с оконечными устройствами, например, клавиатурой, принтером и т.п. 4. В корпусе монитора. 5. В корпусе клавиатуры. 6. В корпусе принтера.
Способ передачи информации	1. Без передачи информации (перехваченная информация записывается на специальные цифровые накопители - flash-память). 2. По радиоканалу. 3. По сети 220 В. 4. По выделенной линии. 5. По оптическому каналу.
Тип источника питания	1. От низковольтных источников питания технических средств. 2. От сети 220 В.
Вид исполнения	1. Обычные (отдельные модули). 2. Камуфлированные под типовые элементы электронных устройств.
Способ управления передатчика	1. Неуправляемые (с включением передатчика при включении СВТ). 2. Дистанционно управляемые.
Способ накопления информации	1. Без накопления. 2. С промежуточным накоплением (с коротким и длительным временем накопления).
Способ кодирования информации	1. Без кодирования информации. 2. С цифровым шифрованием информации.

Классификация методов поиска ЗУ перехвата информации, внедряемых в СВТ

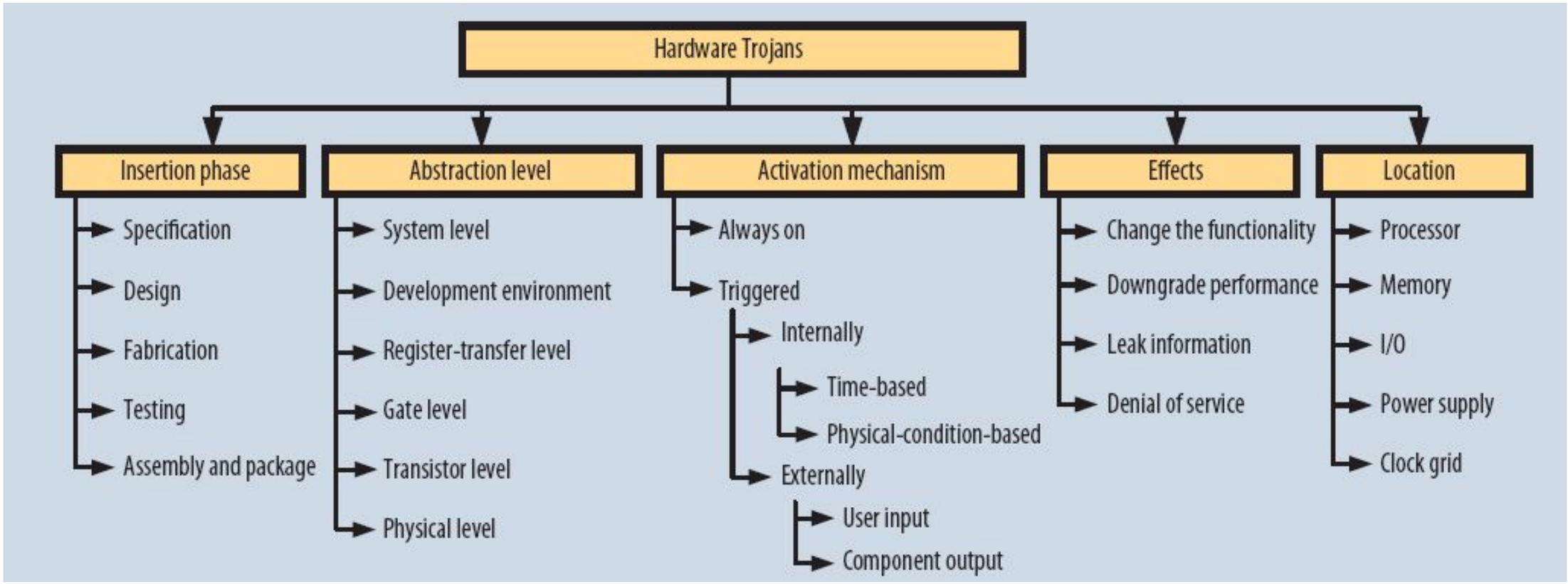
- Специальная проверка СВТ
- Специальная проверка проводных линий
- Радиомониторинг (радиоконтроль) объекта
- Мониторинг (контроль) акустических (виброакустических), оптических и других каналов утечки информации

Классификации Hardware Trojans



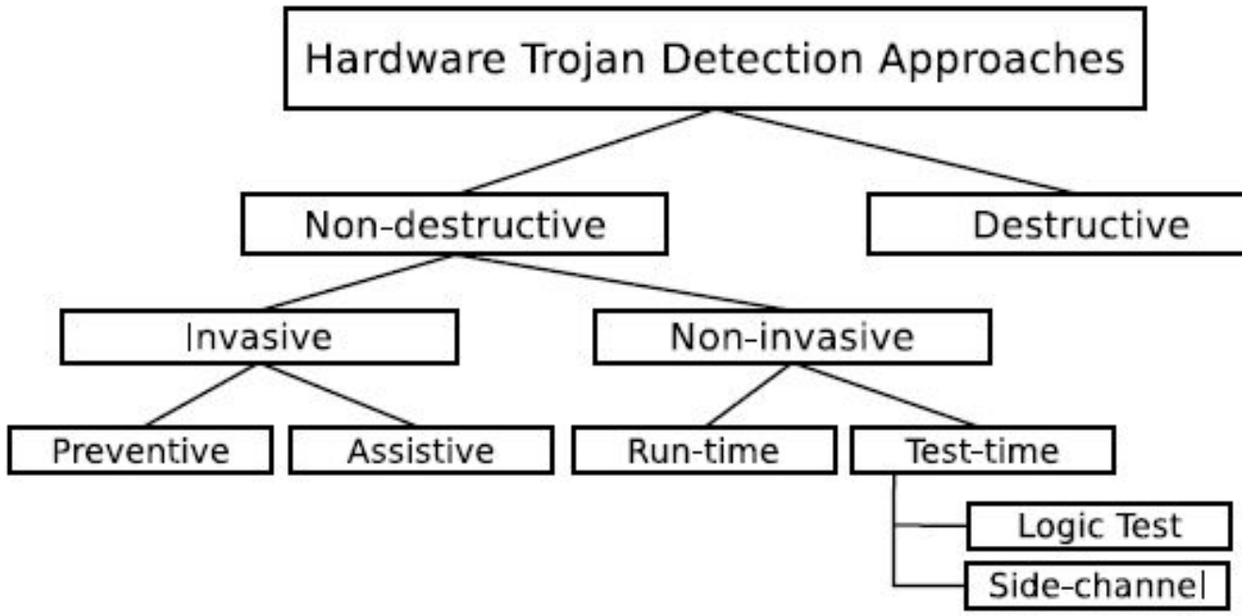
A Survey of Hardware Trojan Taxonomy and Detection // IEEE Design & Test of Computers, 2010

Классификации Hardware Trojans



TRUSTWORTHY HARDWARE: IDENTIFYING AND CLASSIFYING HARDWARE TROJANS // IEEE Computer, N10 2010

Классификации методов поиска Hardware Trojans



Chakraborty, Narasimhan & Bhunia. Hardware Trojan Detection Techniques: (2010)

Классификационные признаки ЗУ

Классификационные признаки ЗУ

- Структурные признаки
  - уровень описания (абстракции)
  - тип реализации
  - размер
  - перекомпоновка
  - плотность интеграции
- Функциональные признаки
  - тип вредоносного действия
  - механизм активации
- Вспомогательные признаки
  - постоянство структуры исходного объекта
  - фаза ЖЦ внедрения
  - фаза ЖЦ активации

Классификационные признаки методов поиска ЗУ

Классификационные признаки методов поиска

- Основные характеристики
  - деструктивность
  - активность
- Вспомогательные характеристики
  - техническая документация
  - встроенные элементы в исходном объекте
  - фаза ЖЦ поиска

Спасибо за внимание

Барановский Олег Константинович
Государственное предприятие «НИИ ТЗИ»