The Developmental Psychology of Intrusion Detection Systems

— Predicting the Future —

Stefan Schumacher

www.kaishakunin.com

DeepSec Security Conference
Vienna, Austria
November 19 – 20 2009

解釈人

About Me

- Student of Educational Science and Psychology at University of Magdeburg/Germany
- Freelance Security Consultant (`www.Kaishakunin.com`)
- Focus on Social Engineering, Security Awareness
- research on Organizational Security
- so I will give no answers, but raise more questions ;-)

解釈人

Background

- every intrusion/security incident has a social dimension
- to detect/prevent security incidents, the social dimension has to be analysed
- anticipate future events
- behaviour at $t_n \rightsquigarrow$ *predicted* behaviour at t_{n+1}
- this is a probabilistic decision
- diagnostic and prognostic competences, social intelligence
- cognitive faculty (*gnosis*) is required
- core competencies of psychology and psychiatry

解釈人

non-technical IDS

- current interesting research (beyond computer science):
- prevent school shooting and identify potential school shooters (University of Berlin)
- analyze surveillance cameras to identify potential terrorists
- also: criminal prognosis, criminology

解釈人

decisions and decision making

- Heinz von FÃ¶rster: Metaphysical Postulate
- there are two kinds of decisions:
- those wo already have been made
- those wo cannot be made
- 1st: is the earth center of the universe?
  geocentric model ./. heliocentric model
- 2nd: should gay marriage be allowed?
- 1st: verification of a computer programm (check for buffer overflows)
- 2nd: is the behaviour of Mr. X just friendly or is he conducting social engineering?

解釈人

Developmental Psychology?

- swiss Biologist Jean Piaget (1896 – 1980)
- interested in how humans generate cognition/gnosis
- analysed children and their development
- created a theory of Â»genetic epistemologyÂ«
- big influence on developmental and pedagogical psychology
- described developmental steps of children
- development of the mind of children

解釈人

Developmental Psychology!

use the genetic epistemology to create a theory of intrusion detection that has diagnostic and prognostic competences, social intelligence and cognitive faculty

解釈人

The Genetic Concept

- Darwin introduced the concept of Development as Evolution/Epigenetics
- Evolution is a Process that builds *new* Structures and Attributes from indifferent Genes
- new capabilities are developed
- Evolution has no determinable beginning and no defined end
- Ontogenesis: evolution of one human being
- Phylogenesis: evolution of one phylum (eg. whole mankind, science)

解釈人

Structure

- central theoretical concept of genetic Epistemology
- nucleus of development
- predetermine direction of development
- inspired by biological concept of holism
- led to genetic psychology
- and cybernetic theory of equilibration
- structures describe cognition via general forms
- and gnosis via its internal schema
- structures describe how cognition is organized

解釈人

Structure

- Piaget defines the human mind as organism, which is differentiated from the environment (the whole) but interacts with it
- Structures are in general Systems of interrelations between their elements and between the elements and the Whole
- non static
- self-organizing
- The whole is more than the sum of its parts.
- cognition is more than the sum of single perceptions
- a structure can be used on Thinking & World, Mind & Matter
- each structure is a momentum of an uncompleted *and* uncompletable process of construction

解釈人

Assimilation & Accomodation

- how are structures created/updated?
- basic structures are created by Â»hardwareÂ« (brain, CPU)
- structures assimilate objects
- objects accomodate structures
- Assimilation: subjective structures are used on objects, which are assimilated into the structures
- Accomodation: objects accomodate structures
- Assimilation and Accomodation are mutually dependent
- each action invokes Assimilation and Accomodation
- perception organizes external events with existing perception structures

解釈人

human development









解釈人

Learning Motivation

- Piaget developed no explicit motivational theory
- Structures shall be kept equilibrated
- equilibrated structures are failure resistant
- non equilibrated structures cause cognitive conflicts
- structures are liberated step by step
- each higher structure is more comprehensive than its predecessor

解釈人

reflective Abstraction

- cognition is more than collecting data
- reflective abstraction uses reflection and construction
- people have to reflect about the structures they are using
- and how they are influencing experience and cognition
- after reflection, new structures can be build
- any developmental process is influenced by older structures

解釈人

Consequences

- epistemology leads to (some kind of) identity
- each IDS will be unique $\rightsquigarrow$ incomparableness
- one IDS might detect an intrusion, another might not
- asset diagnostic required
- an epistemic IDS might be able to detect new attacks (it has the learning potential to learn the skills required to detect attacks)

解釈人

Learning

- Â»realÂ« learning is required to achieve proficiency in ID
- learning *always* requires a feedback loop
- one cannot learn from an unidentified attack
- so we still have the diagnostical problem

解釈人

Learning Theory: Behaviorism

- influenced by Pawlow
- B.F. Skinner: Operant Conditioning with Rats, Cats, Dogs
- Norbert Wiener: Theory of Cybernetics
- Learning as a simple Stimulus/Response Mechanism

teach information
give the learner time to understand
ask a question on the subject taught
give feedback based on the quality of the reaction
repeat

解釈人

Model of a working IDS in training



解釈人

my current working hypotheses

- security is a social problem
- only humans are able to detect intrusions
- computers can make no decisions
- computers are just tools
- security is a dimension of organizational culture
- more organizational research has to be done
- a theory of organizational security is required

解釈人

Questions?
Stefan.Schumacher@Kaishakunin.com

解釈人