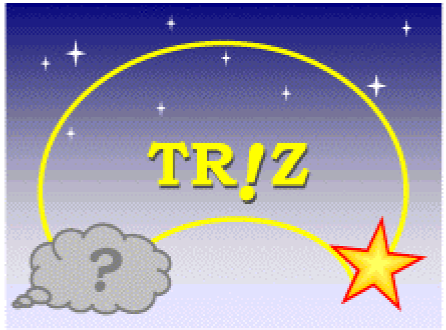
The Fifth TRIZ Symposium in Japan, 2009
Held by the Japan TRIZ Society, NPO



TRIZ/USIT Case Study:
How to Help Recall Passwords

Yutaro Ueda*, Hiroki Nabeshima*,
and Toru Nakagawa
(Osaka Gakuin University)
* 4th Year Student, Faculty of Informatics

September 10-12, 2009
National Women's Education Center, Japan (NWEC)
(Ranzan-machi, Hiki-gun, Saitama Prefecture, Japan)

Outline of Presentation

- **Nakagawa's Seminar Class: "Creative Thinking for Problem Solving"**

  Small number of students (5 to 1 depending on the year)

- **"How to Help Recall Passwords"**
- **Group practices in the seminar class (2 or 3 students only)**

  - Teacher facilitated the group practice.

  - Students' discussions and remarks were recorded on the white board.

  - The white board records were taken in photos.

- **TRIZ and USIT were used in a flexible manner.**

  - USIT led the solution procedure:

  Problem definition, Analysis of the present system (Function & Attribute analysis),
  Image of the ideal system, Idea generation,

  - TRIZ helped the idea generation:

  Physical Contradiction, Idea generation with 40 Inventive Principles

  - A system of solutions is built up with TRIZ and USIT

Problem Situations

- We have many opportunities to use Passwords in everyday life as well as with PCs.
- We need to handle many, different Passwords.
- We can decide the Passwords in some cases, but we are given the Passwords in many other cases.
- We can not remember all the Passwords by heart, so we need to record and manage them properly.
- If a Password is leaked to a malicious person, we are in a serious risk of damage.
- We want to find a proper way to manage a large number of Passwords and to help recall them.

Problem Definition: "How to Help Recall Passwords"

(1) ID/PWs may be decided for ourselves in some cases,
while they are given by the system in some other cases.

(2) When we may decide, how should we decide the PWs?

How can we help ourselves recall them?

(3) When the PWs were given to us (often in complex forms),
how can we help ourselves recall them?

(4) Even if the Hints are stolen, they must not tell the PWs to others.

How should we make the Hints and manage them safely?

(5) The media of the Hints are sheets of paper, primarily.

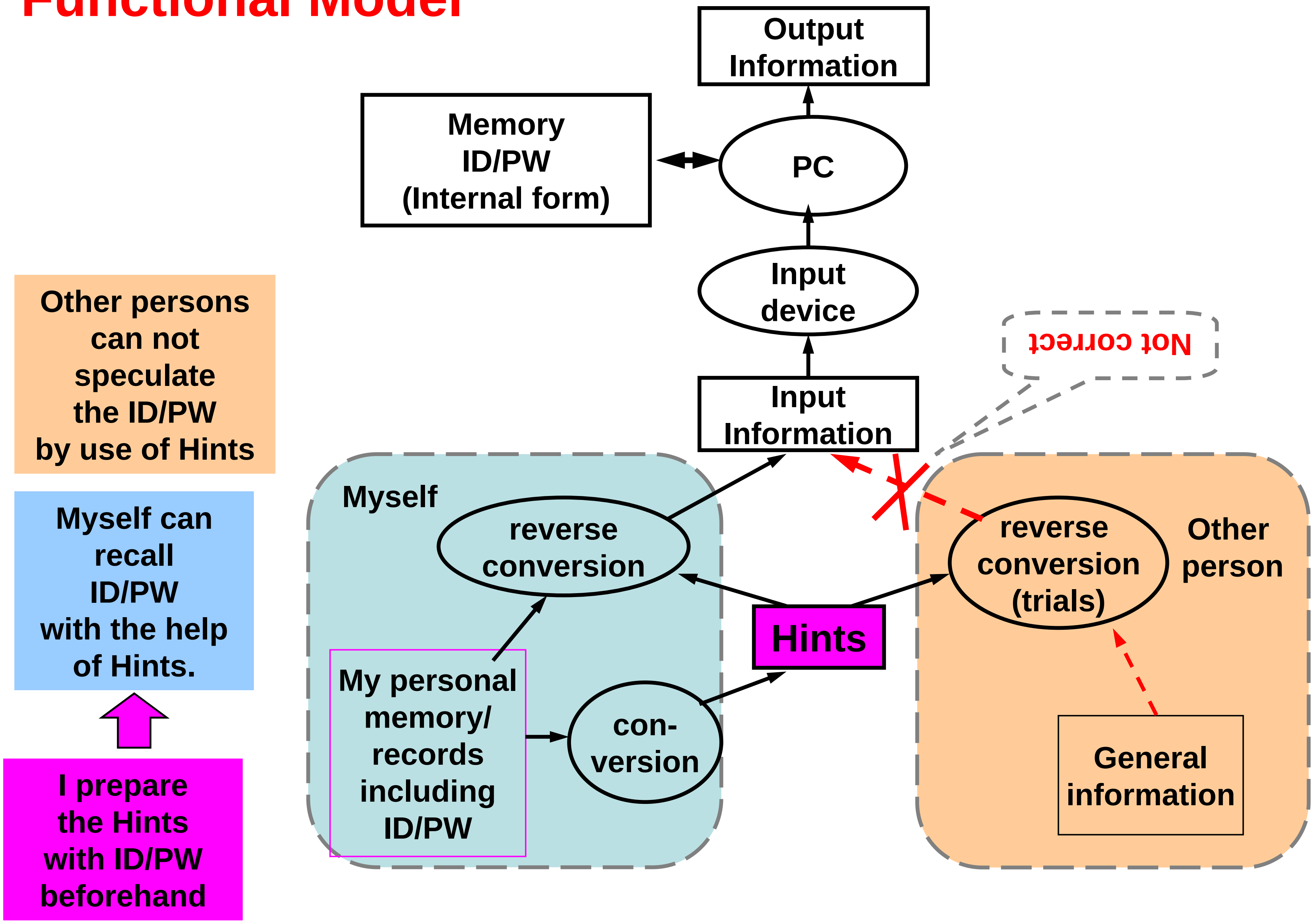
Methods of storing them in PCs/cell phones will be considered later.

(6) If one cannot recall the PW by any means, a new PW will be issued.

The process of PW re-issuing is already established.

-- It's outside of our problem.

Functional Model



Output Information

Memory ID/PW (Internal form)

PC

Input device

Input Information

Not correct

Myself

reverse conversion

My personal memory/ records including ID/PW

con- version

Hints

reverse conversion (trials)

Other person

General information

Other persons can not speculate the ID/PW by use of Hints

Myself can recall ID/PW with the help of Hints.

I prepare the Hints with ID/PW beforehand

Attribute Analysis

What kind of properties should have the PWs and Hints?

Attributes of PWs and Hints:

(a) Attributes of PW/Hints, as a concrete medium

Recorded medium, way of recording, way of carrying, etc.

⇨ (Mostly) related to the degrees of risks of
passing to or being read by other persons

(b) Attributes of PW/Hints, as information (or signals)

Number of characters, character set, regularity, meaning, etc.

⇨ (Mostly) related to the degrees of risks of being the PW
speculated by other persons after having been
passed to or read by them.

How easy to recall/speculate the original PW by use of the Hints?

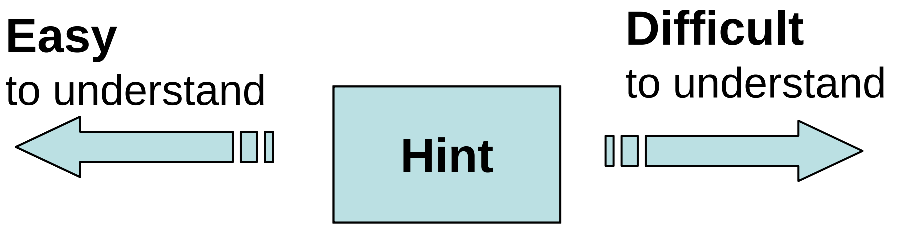
==> The most critical issue of the present problem

Various Attributes of PW/Hints, as the information (or signals)

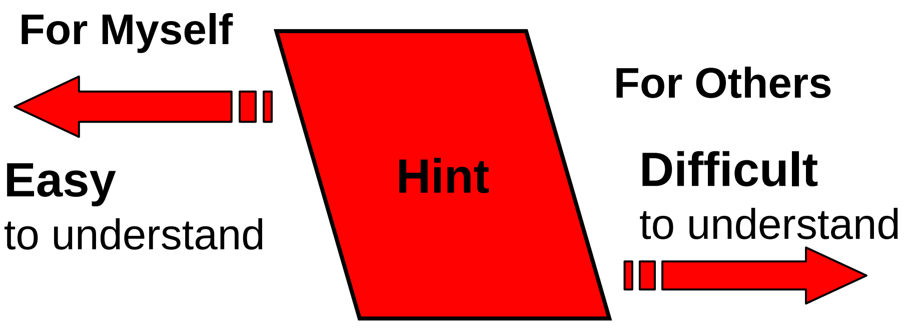
Easiness of understanding the PW	"Easy to Understand"	"Difficult to Understand"
	Easy to remember the PW, Easy to recall PWs with the Hints, Easy to speculate PWs with the Hints	Difficult to remember the PW, Difficult to recall PWs with the Hints, Difficult to speculate PWs with the Hints
Simplicity	Simple	Complex
number of digits/ characters	4 up to 7±2	8 16 （credit card number） 24 (software key number)
character set	numbers (10 characters） English alphabets (26 characters) alpha-numerical (36)	alphanumerical + special symbols (46) alphanumerical + upper case letters (62 characters)
regularity	Some regularity involved: e.g. 1111…, 123…, ….321, 121212…, abcdef…, abcd 1234 efgh 5678	Without apparent regularity: (remove any regularity) irregular in the order, mixed randomly, at random by using random numbers

Word	• in a word • in a simple sentence • composed in a sequential manner • in a word-chain	▪ composed with a few words • characters are interchanged in a word • nonsense sentence • words are intermixed • word-chain in the middle of words
Meaning	• my own Information • easy, commonly-used words (nouns, proper nouns) • favorite words, favorite things • a group of words	• unfamiliar words (in Russian, in Italian) • special words (special term, small local place, dialects) • words outside of ordinary association
Relation with other PW	• in the same pattern • changed in a part • some connection in the meaning	• different, independent patterns • changed in multiple parts • arranged irregularly
Hierarchy of PWs	PW in one step	PWs in multiple steps (After entering with a PW, another PW is requested)

Making the hints
Easy to understand or
Difficult understand
is not a solution either.

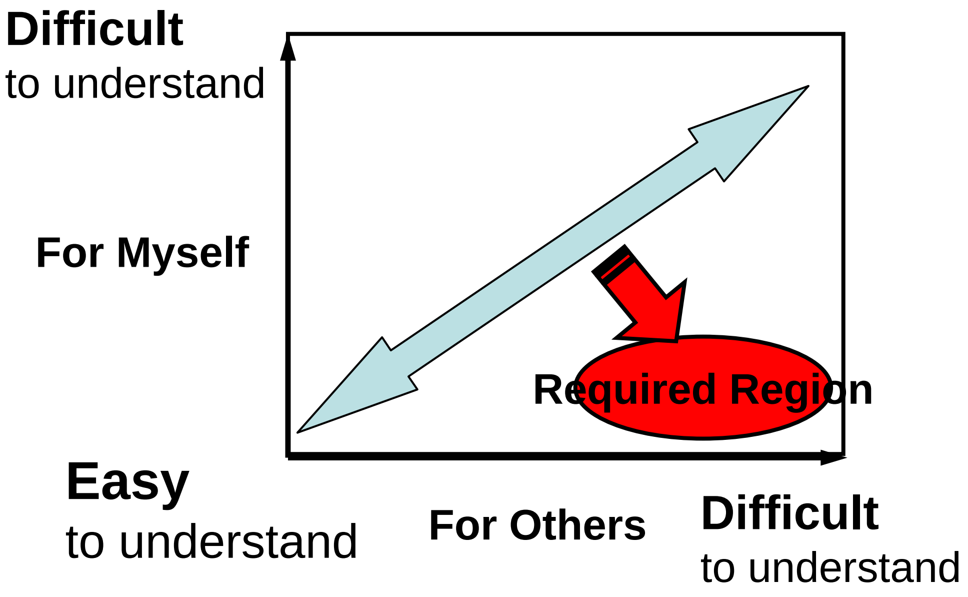


The requirement of this problem is: ==>



This is a case of
Physical Contradiction
in the TRIZ terms.

The contradiction
need to be solved with
the Separation by
the Subject of the Action.

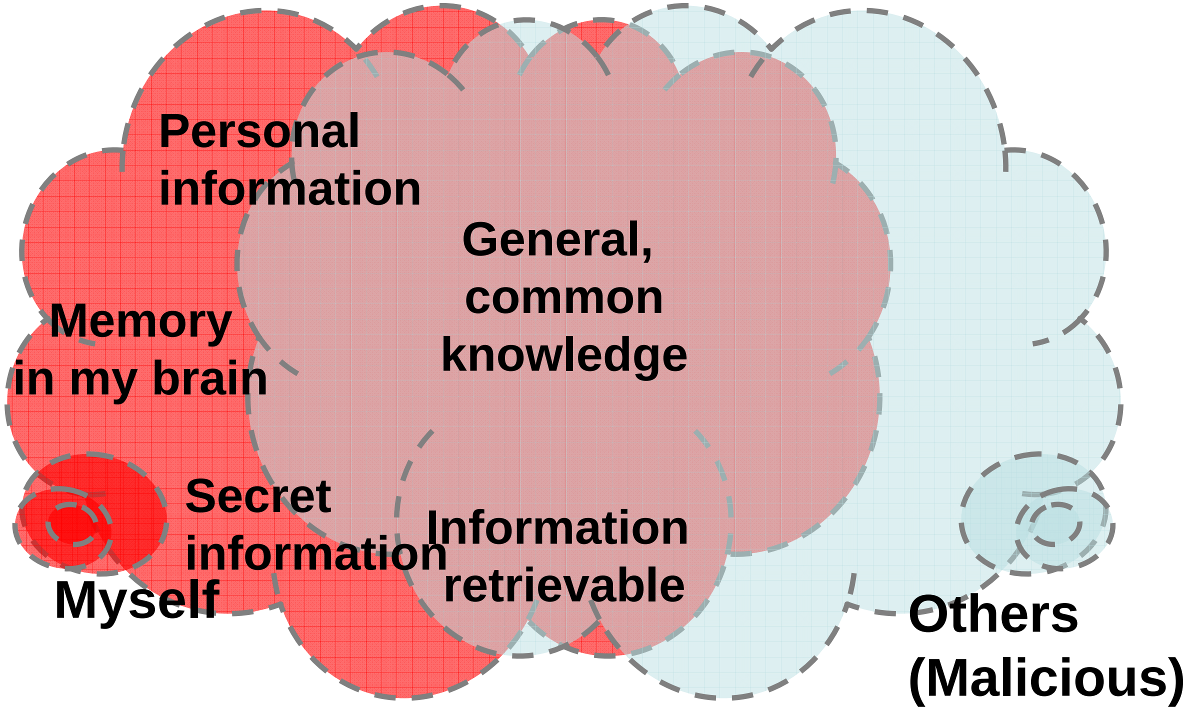


Myself vs. Others
(Model of knowledge)

"Malicious people" are
the persons
in the present problem.

Hence, the area of
the information
which only myself know
is rather small

and is getting
smaller and smaller
due to their invasion...



Personal information

General, common knowledge

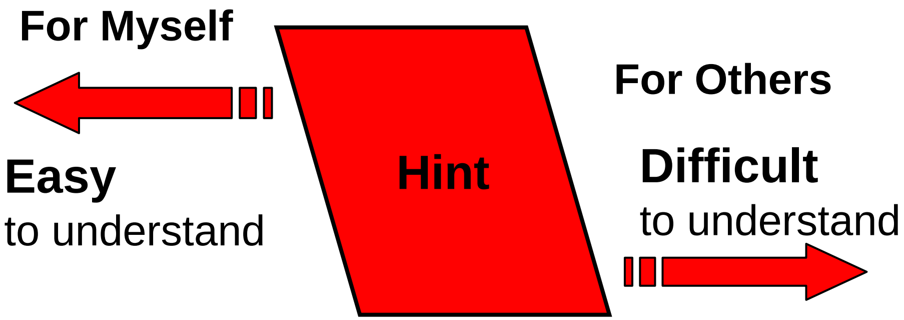
Memory in my brain

Secret information

Information retrievable

Myself

Others (Malicious)



For Myself

Easy
to understand

Hint

For Others

Difficult
to understand

On the basis of these analysis, we tried to generate solution ideas by using the 40 Inventive Principles in TRIZ. Then, we reorganized them to obtain the following solution principles:

Principal Solution Directions:

(1) Handle the PWs we set ourselves separately/differently from those given to us, concerning to how to make and carry the hints.

(2) Insert dummy information intently and frequently in the Hints.

(3) Make a unique, non-universal, non-uniform conversion method and use it for generating the Hints.

(4) Apply relatively simple unique conversion methods in two steps for making the Hints from the PWs.

(5) Keep the information for the reverse-conversion method separately in a secret way.

(6) Use these solution directions together in combination.

(1) Handle the PWs we set ourselves separately/differently from those given to us.

PWs we set ourselves

How to make the PW itself is the main issue in this case.

Choose the PW easy to remember for myself, but difficult to speculate for others.

PWs can be remembered by heart, in most cases.

--> Hints should be much simplified, mostly with the association in meaning.

PWs given to us

PW is given by the system independent of our preference

Often randomized, complex.
No relation among the characters.

Impossible to remember these PWs.
Necessary to reproduce all the characters individually.

--> Cannot omit the PW information in the Hints.
No use of meaning association.

(2) Insert dummy information intently and frequently in the Hints.

PWs we set ourselves

For myself:

Hints may be short and simple.

Insert short Hints into abundant dummy information.

For others:

Difficult / impossible to distinguish the Hints from dummy information.

PWs given to us

Comparison with PW information: 、

・Hints with reduced information:
→ Not enough to recall the PW for myself.　No good.

・Hints with corresponding information:
→ Easy to understand for myself and easy to speculate PWs for others.　No good.

・Hints with extra information:
→ Removing dummy is easy for myself, but difficult for others.
→ Good policy.

(3) Make a unique, non-universal, non-uniform conversion method and use it for generating the Hints.

PWs we set ourselves

In setting the PW, do not use ordinary (universal) words, nor regular (uniform) patterns.

Create a new (unique) word. Generate PWs randomly, and select one easy to remember with some association.

Generate the Hints by use of association (conversion) of meaning.

Not ordinary (universal) association, but case-by -case (non-uniform) association for each PW.

PWs given to us

Conversion from PW to Hints is the principal issue in this type of PWs.

Ordinary (universal) conversion makes the reverse conversion (Hints -> PW) easy, thud dangerous.

Applying conversion partially makes non-uniform (localized) conversion. (Inserting dummy gives non-uniform effects.)

Non-universal and non-uniform conversion makes a unique one. Thus, difficult for others to speculate PW.

(4) Use relatively simple unique conversion methods in two steps for making the Hints from the PWs.

PWs we set ourselves

Apply associative conversion to PWs in two steps to make he Hints

PW --(associative conversion) ->
--(associative conversion) ->
Hints

Difficult to make a unique Hint in one step of association.

Easy to make unique, different Hints in two steps of association.

Easy for myself to remember, but difficult for others to speculate.

PWs given to us

Apply relatively simple conversion to PW in two steps to get Hints.

PW --(conversion 1) -->
--(conversion 2) --> Hint

Each step of conversion may be rather simple.

Insertion of dummy is an example of such an easy conversion.

Localization is another example of easy conversion.

(5) Keep the Information for the reverse-conversion method separately in a secret way.

PWs we set ourselves

Easy to remember PWs and Hints, in this case.

Hints may be sufficient for help recall the PW.

PWs given to us

Difficult to remember the method of reverse conversion from Hints to PW, even if Hints are given.

==> Need to have a memo of the reverse conversion method.

The memo need to be encoded in some secret manner.

We should carry the memo separately from the Hints.

(6) Use these solution directions together in combination.