# Analyzing DNS Incidents

I Made Wiryana - Avinanta Tarigan
RVS Arbeitsgruppe

December 17, 2002

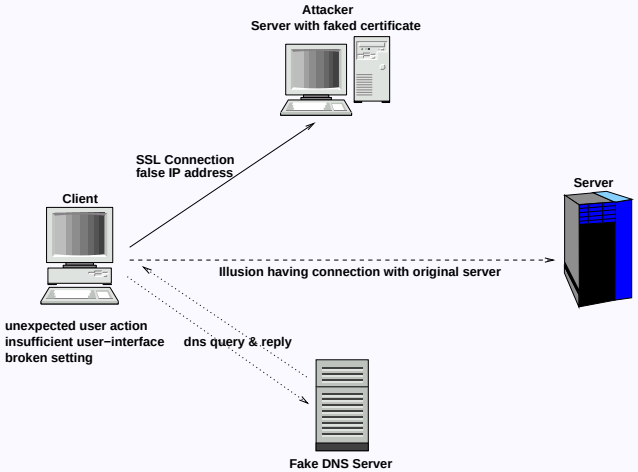
# 1. Internet Banking

- Home banking is already available since 1980.
  - BTX with CETP protocol (Germany), ETEBAC (France). Using direct connection to the bank without encryption.
  - Using PIN/TAN as the authentication mechanism
  - Chaos Computer Club (CCC) had demonstrated the vulnerability of BTX.
- Internet banking
  - Online banking via insecure communication link. Using HTTP + SSL
  - Some proprietary solutions exist, eg. : using java applet, one time password with calculator.
  - Weak cryptography algorithm problem (RC4 with 40 bit)
- Home Banking Computer Interface (HBCI) Standard is developed `<http://www.hbci-zka.de>`
  - Between homebanking software (user computers) and server in the bank. Port 3000 TCP.
  - Between homebanking software and secure storage (smart card)
  - Multibank, dialog oriented based on ZKA-Dialog. It is only a specification
  - Trojan and virus (Backorifice, PCAnywhere) are still threat.
- Other standards :
  - Open Financial Exchange (OFX), Microsoft, Intuit and Checkfree - `http://www.ofx.net`
  - Interactive Financial Exchange (IFX), Banking Industry Technology Secretariat - (BITS) - USA - `http://www.bitsinfo.org/ifx`

# 2. Some Internet Banking attacks

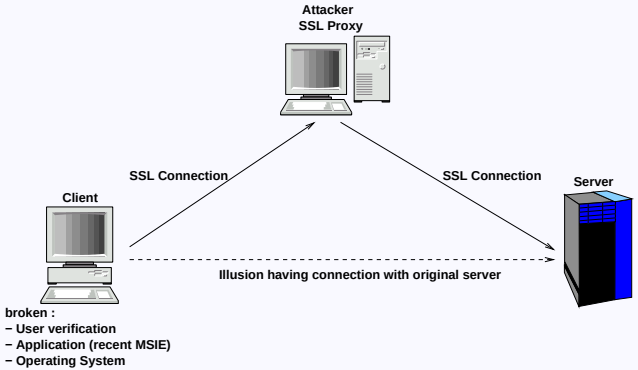
## 2.1. DNS spoofing

- DNS poisoning (exploiting some DNS vulnerabilities)
- DNS server produces the false IP number when there is a request.
- Users connect to the false machine



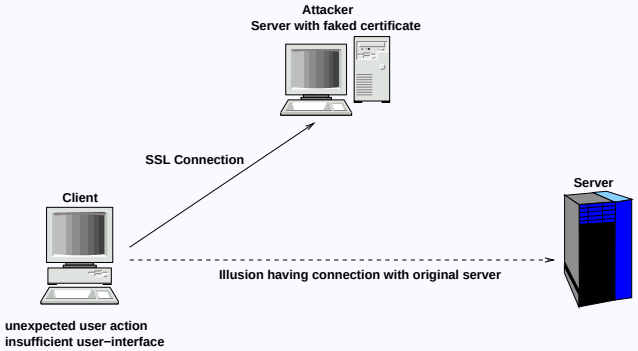
## 2.2. Man in the middle attack

- Using the sequence number prediction. The TCP connectian between user and the bank server can be hijacked.
- Users believes that he/she connects to the real server.
- Both techniques are not easy and require extra technical know-how and cost.



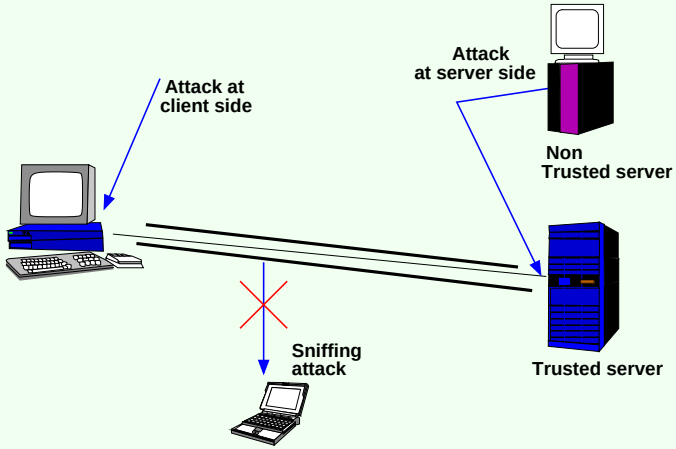
## 2.3. Mistypo attack

- People often mistype the site names.
  - Using the characters that appears similar. `paypal.com` -> `paypa1.com`,
  - Using the typo names. `yahoogroups.com` -> `yahoogroup.com` etc
- Many designers and also USERs are not aware of this problem.
- It is impossible to registered all possible domain names.



# 3. SSL and users

- SSL only protects from the sniffing attack. Many customer are never informed about it.
- User has to guarantee that the host is the original (Certificate Authority plays the main role)
- User have to proof by themselves that :
  - Certificate is issued by a trusted CA
  - Certificate is issued by the correct company (trusted company)
  - Certificate is still valid (`www.ga-citylink.com` problem)



# 4. BCA Incident

## 4.1. Incident description

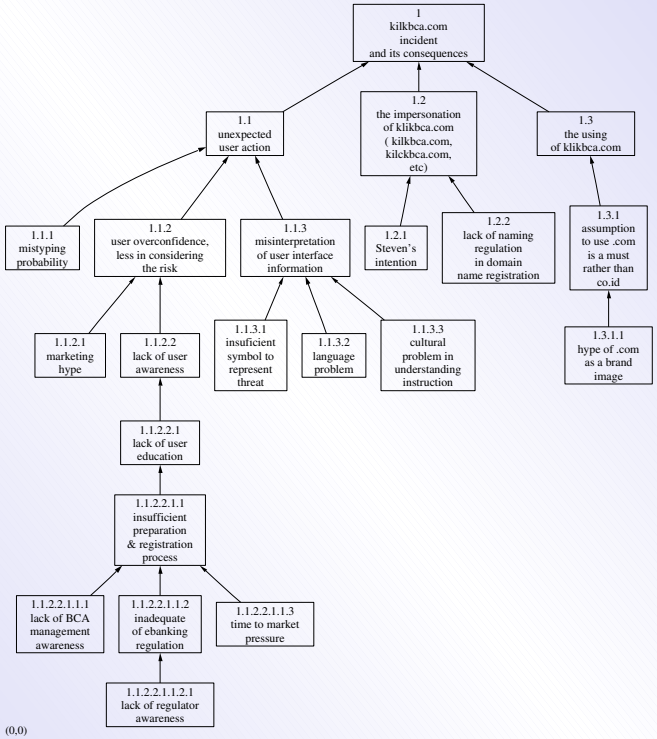
- BCA launched the Internet Banking without enough user education period.
- BCA ensured the security using "*marketing hype*" such as firewall and 128 bit SSL.
- BCA uses `*.com` domain rather than `*.co.id`. Registration process is different.
- BCA did not registered "mistyped domains" such as `wwwklikbca.com`, `kilkbca.com`
- A person (Steven Haryanto) registered the mistyped domain and set up impersonating sites.
- Many people think that impersonating sites are the original BCA sites. They supply username/password when they are asked.
- None of BCA customer realized this situation and nobody complained to BCA. In 48 hours, there are 130 PIN have been collected.
- BCA only used user/password authentication without TAN. This attack can produce a serious problems.
- Most Indonesia users do not understand the SSL dialog (language and understanding problem).

## 4.2. The registration process

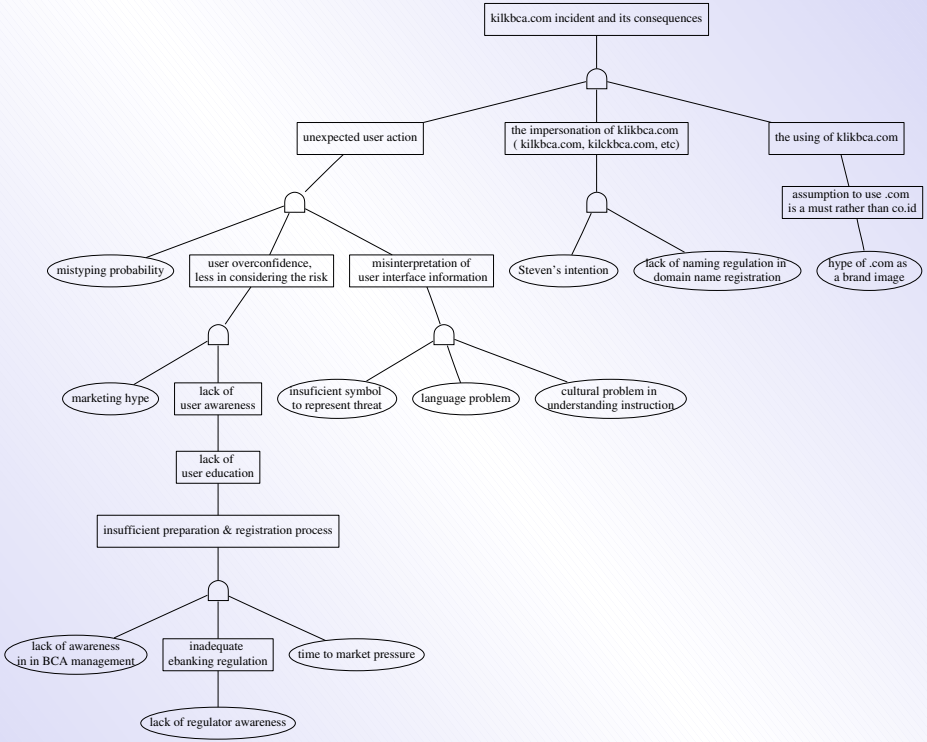
The registration process :

- BCA assumed that users are familiar with Internet Banking
- Every BCA customers automatically can have Internet Banking account and use it.
- There is no formal effort to educate the customer before they use it.

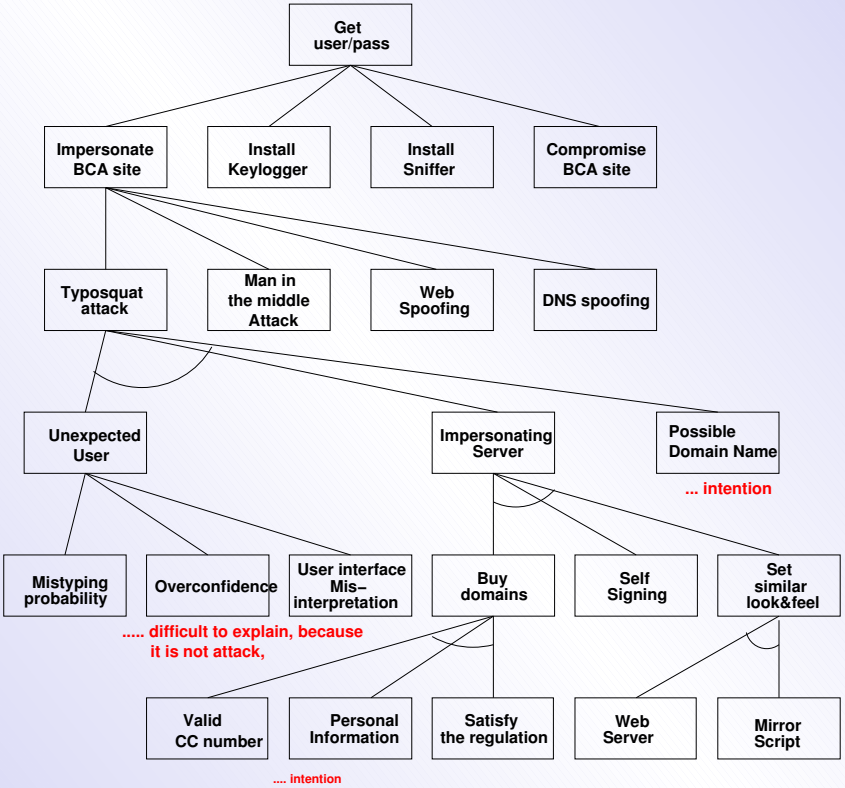
## 4.3. WBA



## 4.4. Fault tree analysis



## 4.5. Attack tree analysis

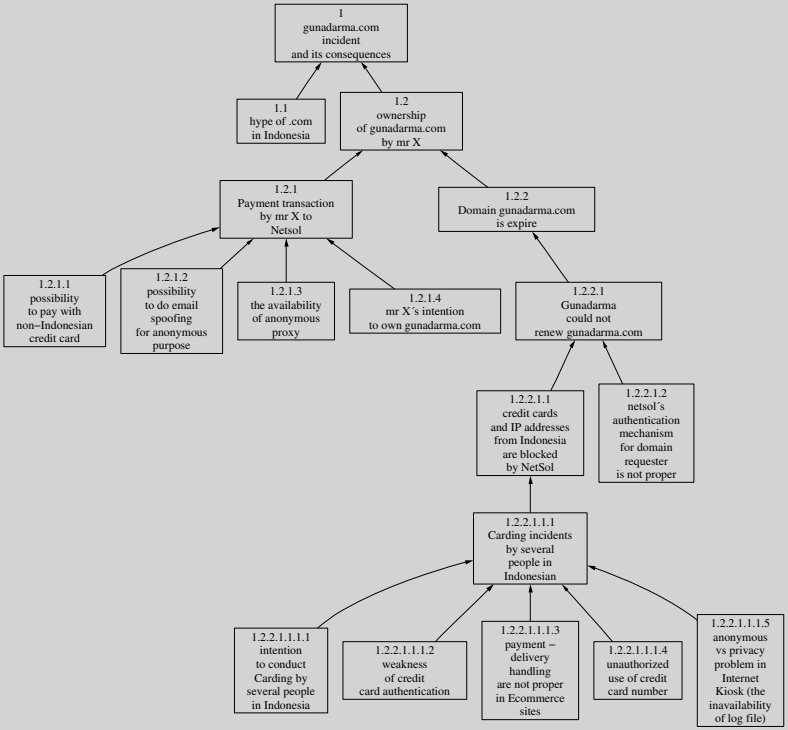


# 5. Gunadarma Incident

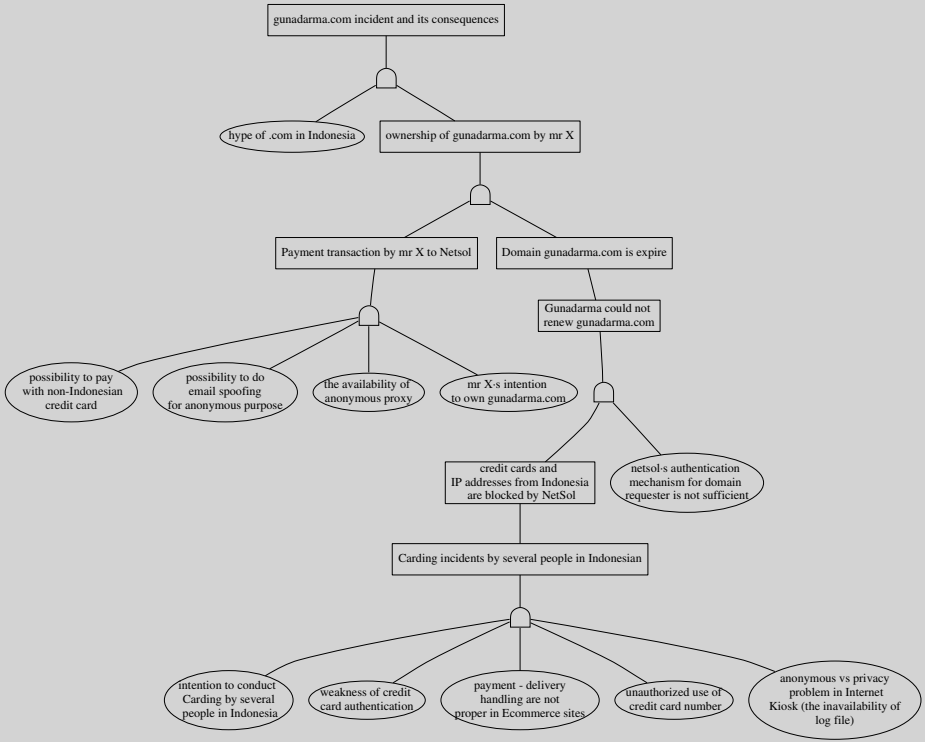
## 5.1. Incident description

- `gunadarma.com` has been registered by one of the Sys Adms in Gunadarma University
- Due to many credit card frauds from Indonesia, the IP and Credit Card from Indonesia are not accepted in some sites.
- Netsol accepted the payment only via credit card. There is no other payment method
- Netsol blocked credit card from Indonesia (TELKOMNET experienced the same problem).
- Gunadarma could not renew the `gunadarma`.com domain
- Somebody (Mr. X) paid the domain used the unauthorized CC. There is no sufficient authentication payment mechanism in Netsol.
- He set up a "sites" (with a similar look and feel but with pornographic contents)
- Many people thinks that the Gunadarma site has been defaced by somebody.

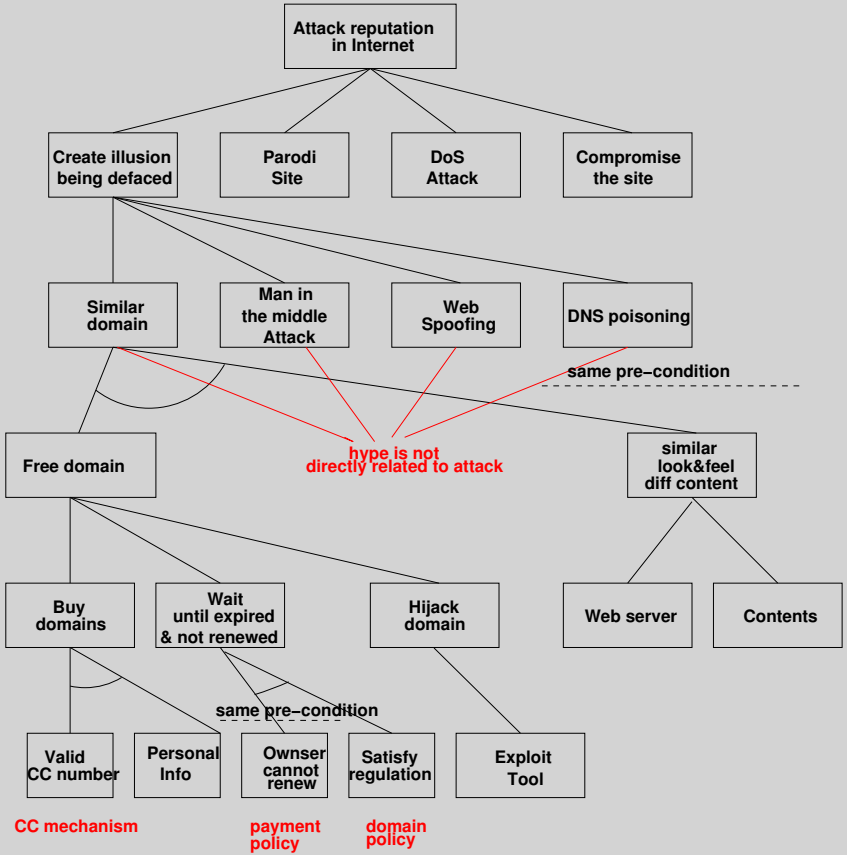
## 5.2. WBA



## 5.3. Fault-tree analysis

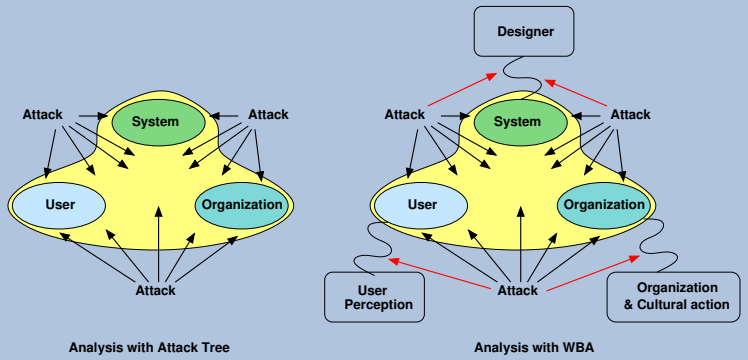


## 5.4. Attack tree analysis



# 6. Discussion

## 6.1. Different attack in the system




Analysis with Attack Tree

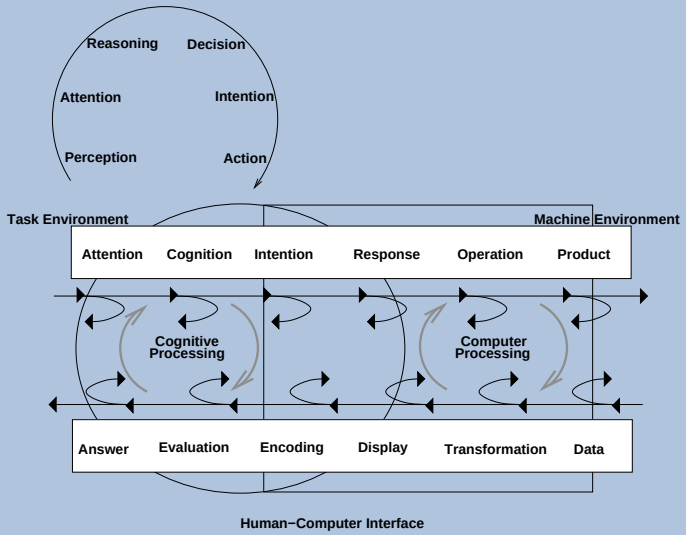
Analysis with WBA

Problem in identifying attack :

- Some attacks are not identified as attack, because it is indirectly related to the system
- The grow of similar attack pattern (nodes in the same level has same pre-conditions)
- Attacks in the link between designer-system, user-system, and organization cannot easily described in attack tree.

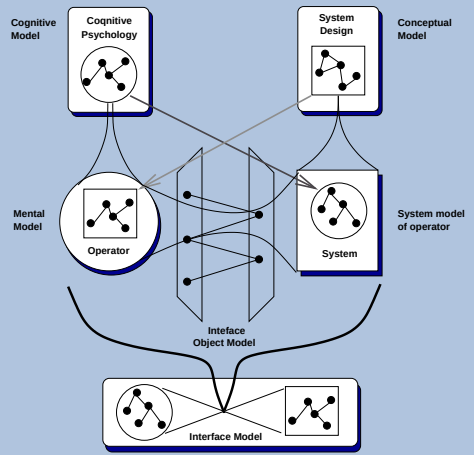
## 6.2. User perception

Flow of information and control at the human-computer interface (Norman et al, 1980). Comparing with the PARDIA model (Ladkin)



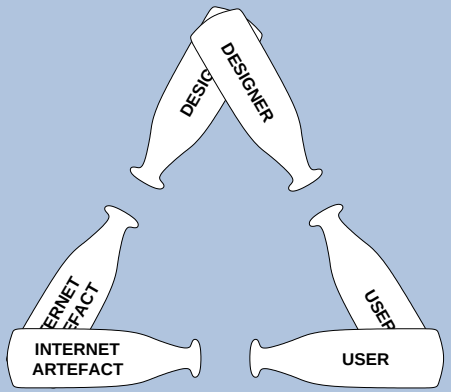
## 6.3. Mental model and system model (Norman)

- **Interface mode** is a representation of the top level specification of the function of the human computer interface
- **Cognitive mode**l is a model of the operator generated typically by a cognitive model
- **System model of the operator** is a representation of the operator's expected processing that is used by the system to predict the user behaviour.
- **Operator conceptual model** is a representation of the system formulated by the designer and given to the operator to aid in the understanding and use of the system.
- **Operator's mental model of the system** is a representation within the mind of the operator of how the system works.
- **Interface object models** are graphical or symbolic representations of token objects.



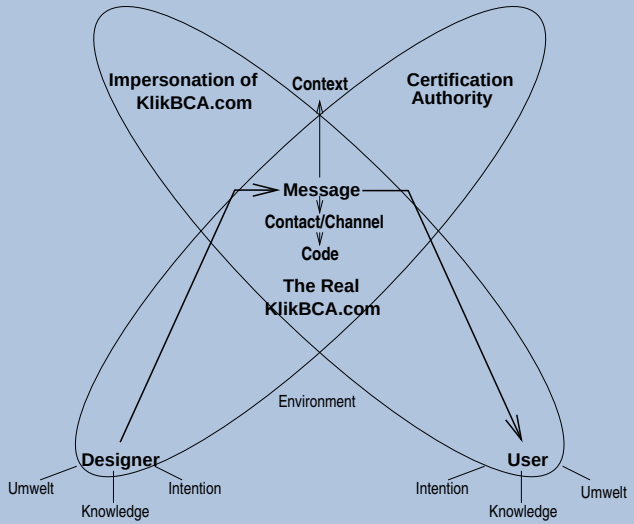
## 6.4. Bottleneck in designing system (Thimbleby)

- Internet-based Software Artefact (IBSA), distributed application delivered via the Internet
- Actors in IBSA :
  - Entities that owns the artefacts
  - Entities that use the artefacts
- Different target groups have a different understanding of the propositional content and action modes.
- Designer face situation where their knowledge of and power over the users are both low.



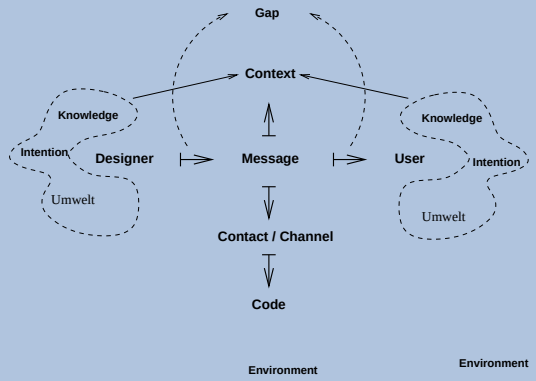
## 6.5. Different boundary of systems

- Designers assume that user knows that the impersonating sites is not part of the system
- However, users think that the impersonating sites is part of the system.
- Designers assume that users check the Certificate properly



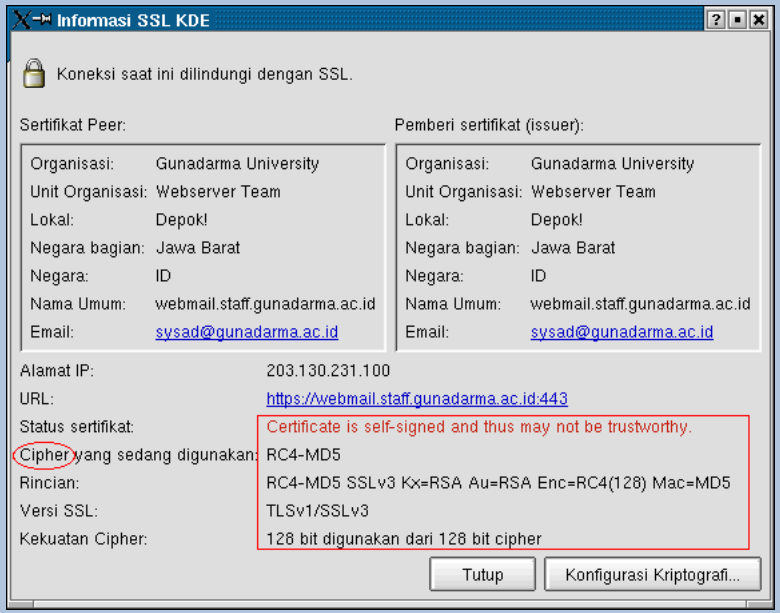
## 6.6. How to communicate the design

- How designers can communicate the design
- How users can understand and have the same system model
- There is gaps between user - designer - artefact.



## 6.7. User Interface and Language


1. Security certificate ?
2. To trust ?
3. Who is the authority ?
4. View certificate ? Some cryptic messages, many users do not understand it
5. **Most users click "YES"**




- Cipher : inappropriate translation
- Too technical information

## 6.8. User education

- Technology solutions are not sufficient for Internet Banking. (For example HBCI attack, Geld-Karte attack).
- There should be a sufficient period in introducing the services.
- The system should be design in order to maintain the security awareness.
- User Interface should be designed with security consideration, not only usability.

## 6.9. Regulation

- How to enforce Internet Banking providers to educate the user
- The accessibility of services (character, language, user interface, dialog model)
- The audit trail : `http://www.ecbs.org`