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, e.g.: 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](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](http://www.ofx.net)
  - Interactive Financial Exchange (IFX), Banking Industry Technology Secretariat - (BITS) - USA - [http://www.bitsinfo.org/ifx](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

![Diagram of DNS spoofing attack](image-url)
2.2. Man in the middle attack

- Using the sequence number prediction. The TCP connection 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.

![Diagram of Man in the Middle Attack](image)
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

1. kikbca.com incident and its consequences

1.1 unexpected user action

1.2 the impersonation of klikbca.com (kikbca.com, klikbca.com, etc)

1.3 the using of klikbca.com

1.1.1 mistyping probability

1.1.2 user overconfidence, less in considering the risk

1.1.3 misinterpretation of user interface information

1.2.1 Steven’s intention

1.2.2 lack of naming regulation in domain name registration

1.3.1 assumption to use .com is a must rather than co.id

1.3.2 lack of naming regulation in domain name registration

1.3.3 cultural problem in understanding instruction

1.1.3.1 insufficient symbol to represent threat

1.1.3.2 language problem

1.1.3.3 cultural problem in understanding instruction

1.2.2.1 lack of user awareness

1.2.2.2 lack of user education

1.2.2.2.1 insufficient preparation & registration process

1.1.2.2.1.1 lack of BCA management awareness

1.1.2.2.1.2 inadequate of ebanking regulation

1.1.2.2.1.3 time to market pressure

1.1.2.2.1.4 lack of regulator awareness

1.1.2.2.1.1.1 insufficient preparation & registration process

1.1.2.2.1.1.2 inadequate of ebanking regulation

1.1.2.2.1.3 time to market pressure

1.1.2.2.1.4 lack of regulator awareness

1.1.2.2.1.5 time to market pressure

1.1.2.2.1.6 lack of regulator awareness
4.4. Fault tree analysis

kilkbca.com incident and its consequences

unexpected user action

the impersonation of klikbca.com (kilkbca.com, kilckbca.com, etc)

the using of klikbca.com

assumption to use .com is a must rather than co.id

mistyping probability

user overconfidence, less in considering the risk

misinterpretation of user interface information

Steven’s intention

lack of naming regulation in domain name registration

deficiency of .com as a brand image

marketing hype

lack of user awareness

language problem

cultural problem in understanding instructions

lack of symbol to represent threat

lack of user education

insufficient preparation & registration process

lack of awareness in BCA management

inadequate ebanking regulation

time to market pressure

lack of regulator awareness

lack of awareness in BCA management

inadequate ebanking regulation

time to market pressure

lack of regulator awareness
4.5. Attack tree analysis

Get user/pass

- Impersonate BCA site
- Install Keylogger
- Install Sniffer
- Compromise BCA site

- Typosquat attack
- Man in the middle Attack
- Web Spoofing
- DNS spoofing

Unexpected User

- Mistyping probability
- Overconfidence

- User interface Mis-interpretation
- Buy domains
- Self Signing
- Set similar look&feel

... intention

Valid CC number

- Personal Information
- Satisfy the regulation
- Web Server
- Mirror Script

... intention

...... difficult to explain, because it is not attack,
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

gunadarma.com incident and its consequences

1.1 hype of .com in Indonesia

1.2 ownership of gunadarma.com by mr X

1.2.1 Payment transaction by mr X to Netsol

1.2.2 Domain gunadarma.com is expire

1.2.1.1 possibility to pay with non-Indonesian credit card

1.2.1.2 possibility to do email spoofing for anonymous purpose

1.2.1.3 the availability of anonymous proxy

1.2.1.4 mr X’s intention to own gunadarma.com

1.2.2.1 Gunadarma could not renew gunadarma.com

1.2.2.1.1 credit cards and IP addresses from Indonesia are blocked by NetSol

1.2.2.1.2 netsol’s authentication mechanism for domain requestor is not proper

1.2.2.1.1.1 Carding incidents by several people in Indonesian

1.2.2.1.1.1.1 intention to conduct Carding by several people in Indonesia

1.2.2.1.1.1.2 weakness of credit card authentication

1.2.2.1.1.1.3 payment – delivery handling are not proper in Ecommerce sites

1.2.2.1.1.1.4 unauthorized use of credit card number

1.2.2.1.1.1.5 anonymous vs privacy problem in Internet Kiosk (the inavailability of log file)
5.3. Fault-tree analysis

Gunadarma.com incident and its consequences

Ownership of gunadarma.com by Mr X

Payment transaction by Mr X to Netsol

Domain gunadarma.com is expire

Gunadarma could not renew gunadarma.com

Possibility to pay with non-Indonesian credit card

Possibility to do email spoofing for anonymous purpose

The availability of anonymous proxy

Mr X's intention to own gunadarma.com

Credit cards and IP addresses from Indonesia are blocked by Netsol

Netsol's authentication mechanism for domain requester is not sufficient

Carding incidents by several people in Indonesia

Intention to conduct Carding by several people in Indonesia

Weakness of credit card authentication

Payment - delivery handling are not proper in Ecommerce sites

Unauthorized use of credit card number

Anonymous vs privacy problem in Internet

Kiosk (the inavailability of log file)
5.4. Attack tree analysis

- **Attack reputation in Internet**
  - Create illusion being defaced
  - Parodi Site
  - DoS Attack
  - Compromise the site

- **Similar domain**
  - Man in the middle Attack
  - Web Spoofing
  - DNS poisoning

- **Free domain**
  - Buy domains
    - Wait until expired & not renewed
  - Hijack domain

- **Web server**
  - Contents

- **Valid CC number**
  - Payment policy
- **Personal Info**
  - Domain policy
- **Owner cannot renew**
- **Satisfy regulation**
- **Exploit Tool**

- **CC mechanism**
  - payment policy
  - domain policy

- **same pre-condition**
  - hype is not directly related to attack

- **similar look & feel diff content**

- **same pre-condition**

**CC mechanism**
6. Discussion

6.1. Different attack in the system

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 model** 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