AGAINST PHISHING

Sender Certification

When phishing happen…..

Victims receive email that contains malicious website. They are not able to identify the malicious website with the authenticated one. So they take it as the authenticated website, and then they are phished.

The authenticated website?

The malicious website?

They are almost identical except the URL and background program.

New Method: Sender's certification should be verified by the receiver.

How it works?

SENDER CERTIFICATION

If the sender is web administrator:

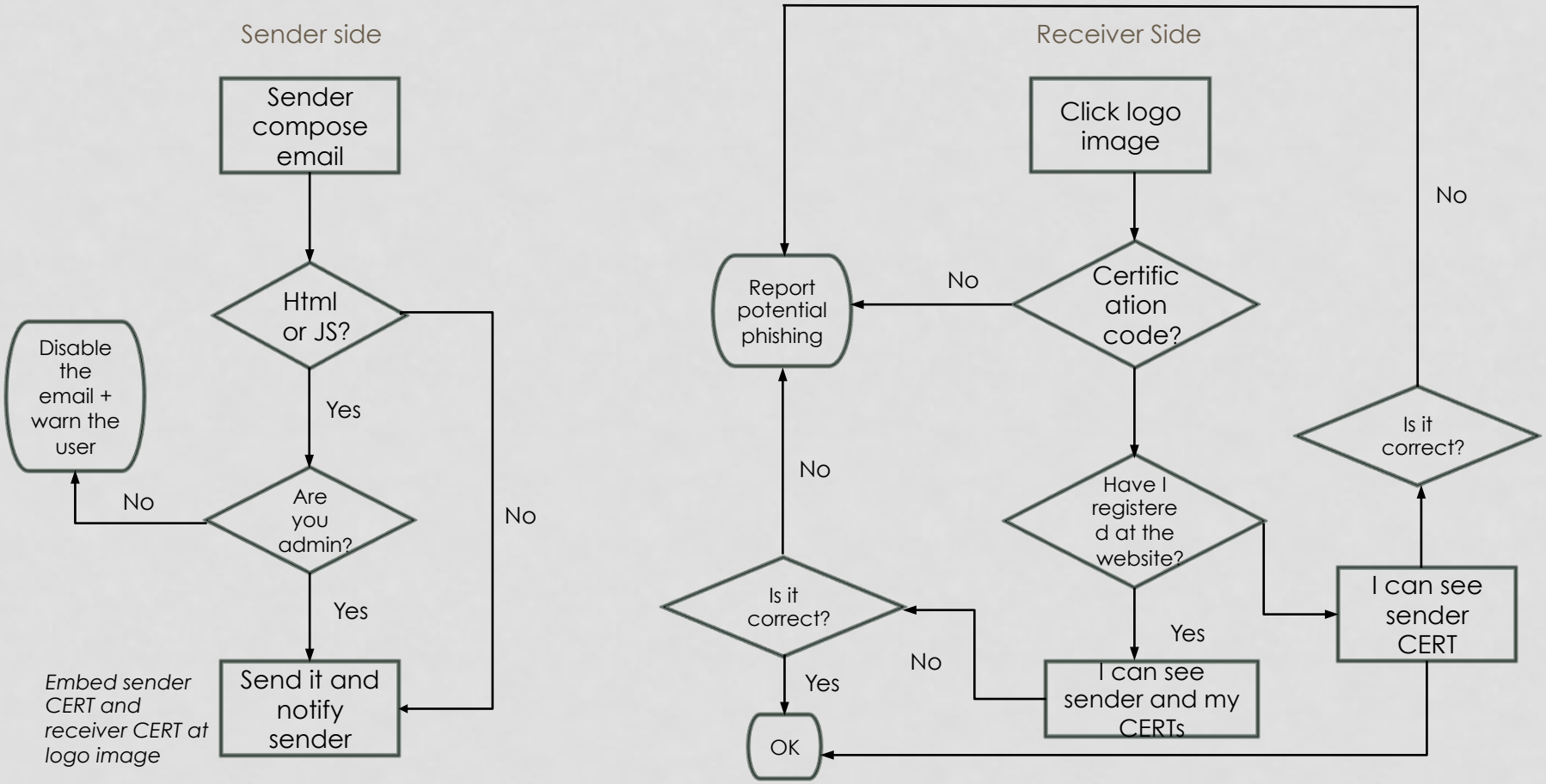
- The sender can send Html or JS as email message.
- The email contains a logo picture which redirects the receiver to verification page.
- The receivers could be either user of the website or non-uses. click the logo picture to see verification code.
  - If the receiver is the user of the website: verification code will be the certification of that user and web administrator.
  - If the receiver is not the user of the website: verification code will be the certification of web administrator.

If the sender is general user:

- Most of steps are same.
- Except the user are not authorized to send Html or JS at email message body.

FLOW CHART

The process to verify sender's identity



POTENTIAL ATTACK

Already fixed

- HTML Injection
- JS Injection
  - Solution: we disable all the outgoing message containing script except the email is from web administrator.
  - Solution: We extract all the URL included at the message body and verify if the URL is trustworthy.
- SQL Injection
  - Solution: trim the user input as string.
- Brute-Force Attack
  - Solution: simply numeric CAPTCHA
- DPA Attack:
  - Registration takes time. Such as required full name, address, phone number, email, and even driver license.

SIGNIFICANCE

Differences with previous research

- Prevent against redirection phishing attack.
  - One way communication.
  - Users can verify sender without sending extra request to sender or the website.
- Verify sender's certification.
- Reduce communication burden.
- Add phishing report mechanism.
  - If the information you see or receive is different from the correct official data, there will be an alert to warn you that you may be phished.

UNSOLVED PROBLEMS

- Doesn't work for the website which don't take registration.
- More advance SQL injection, or other exploit attack method.
- Client Certification.
- Certification exposure.
  - Even thought we send email alert the sender that his certification has been viewed by the receiver, the sender might not pay attention to updating his certification.

REFERENCE

- B. Adida, S. Hohenberger, and R. Rivest, "Seperable Identity-Based Ring Signatures: Theo- retical Foundations for Fighting Phishing Attacks," In submission.
- B. Adida, S. Hohenberger, and R. Rivest, "Fighting Phishing Attacks: A Lightweight Trust Architecture for Detecting Spoofed Emails," Draft, February 2005
- M. Jakobsson, "Modeling and Preventing Phishing Attacks," Phishing Panel of Financial Cryptography 2005.
- M. Jakobsson, S. Myers. "Delayed Password Disclosure to Defend Against Doppelganger Windows Attacks," In preparation.
- V. Boyko, P. MacKenzie and S. Patel, "Provably Secure Password Authentication and Key Exchange Using Diffie-Hellman," EuroCrypt 2000, pp. 156-171.

Thank you

04.30.2015

Snow Zhou

Q & A