Universität Konstanz

HOCHSCHULE DER MEDIEN

A Novel Anti-Phishing Framework Based on Honeypots

Shujun Li[1] and Roland Schmitz[2]
[1]University of Konstanz, Germany
[2]Stuttgart Media University, Germany

Presenter: Junaid Jameel Ahmad[1]

General Members Meeting &
eCrime Researchers Summit
October 19, 20 & 21, 2009 – Tacoma, WA

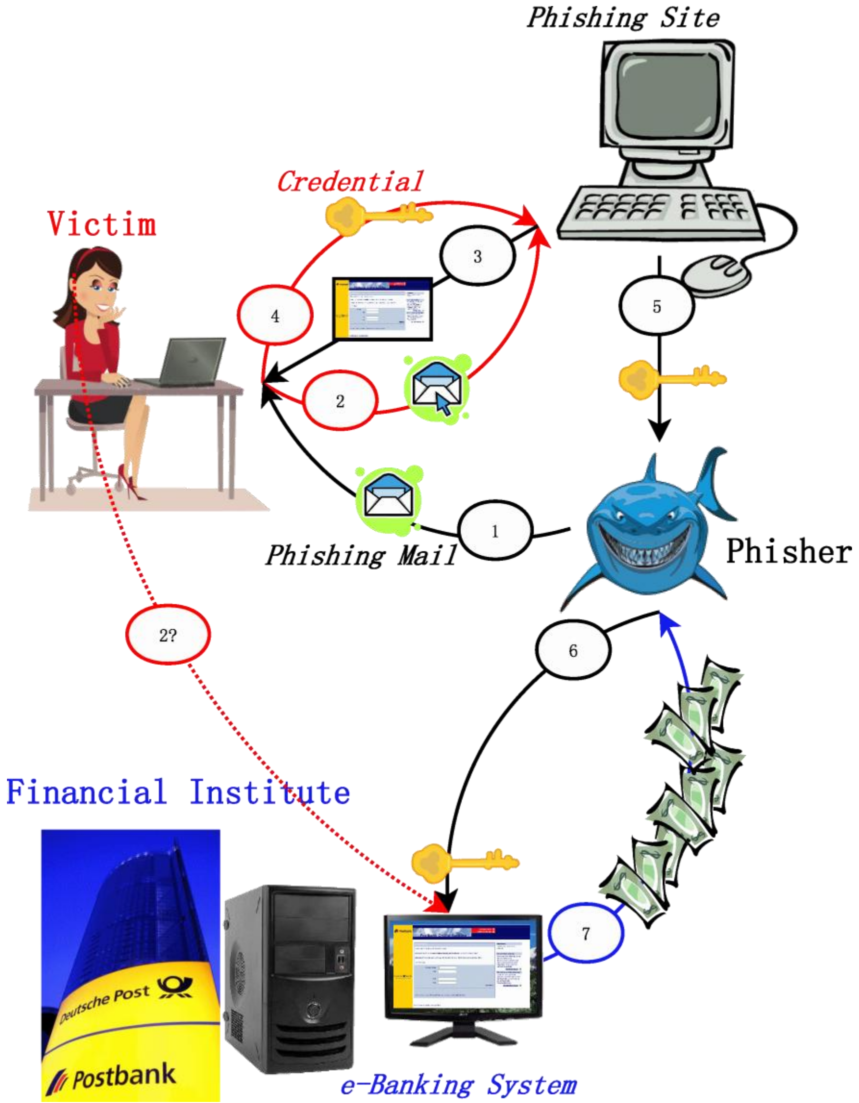
Outlines

- The Phishing Process
- Existing Countermeasures and Limitations

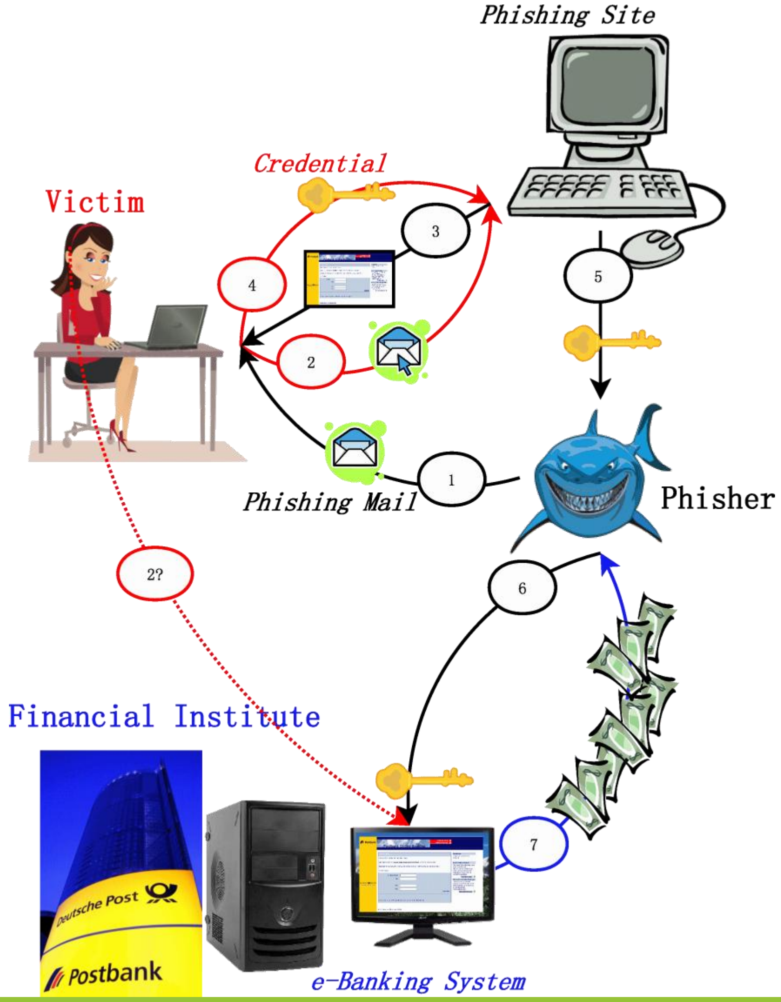
- Existing Anti-Phishing Honeypots: Not Enough?
- *Problems and our solutions* ⇒
- The Proposed Framework

- Summary, or Take-Home Messages

The Phishing Process



Existing Countermeasures



- Step 1: Phishing mail detection, ...
- Steps 2-4: Server authentication, ...
- Step 5: Early phishing site Detection, ...
- Step 6: Two-factor user authentication, ...
- Step 7: Transaction authentication, ...

Common Limitations

- 100% automatic detection rate?
  - No way!

- “Alice, do you really want to go phishing?”
  - Alice: “Yes, I do!”
  - Users are not dependable!

- “Please insert your USB-key…”, or
  “Please install this plugin before continuing…”
  - “Oh no, I already have enough of this …” ☹

Why Honeypots?

- 100% detection rate? – Well, at least nearly 100% should be possible.

- “Hi Alice and Bob, we don’t play with you. We only play with Eve.”

A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource.

Anti-Phishing Honeypots

- Spamtraps = Honeypots against spammers
- Phoneytokens = Honeytoken against phishing
- Phoneypot = Honeypot against phishing = Simulated e-banking system against phishing
  - It works with phoneytokens.

- Commercial anti-phishing honeypots
  - RSA® FraudAction^{SM}
  - MarkMonitor’s Dilution™ and Phish Tagging, …

Anti-Phishing Honeypots: What’s wrong, folks?

- Problem 1
  - Spamtraps--------- ---------Phoneytokens
  - ⇒ Phishers: “Hmm, this does not seem to be from a human user…”

- Solution
  - Spamtraps–Phoneytokens
  - Even better: Spamtraps–Human manager–Phoneytokens

Anti-Phishing Honeypots: What’s wrong, folks?

- Problem 2
  - Phoneytokens can be verified easily if they cannot be used to access the e-banking server.

- Solution
  - Honeying the real e-banking system

  - Phoneytokens can be used for login exactly like real credentials
  - Phoneytokens + Phoneypot (A simulated e-banking system)

Anti-Phishing Honeypots: What’s wrong, folks?

- Problem 3
  - Phisher: “I got 100 credentials. Which ones on earth are phoneytokens?”
  - “Hmm, why not send some cents to a real account as a test?”

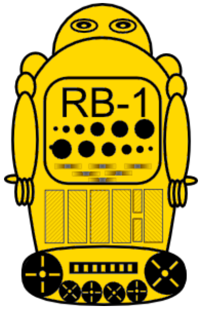
- Solution
  - The e-banking system should be deep honeyed. ⇒
  - Real fund transfer should be supported to some extent.

  - It is just a matter of time…
  - So, our goal is to prolong the lifespan of phoneytoken.

Anti-Phishing Honeypots: What’s wrong, folks?

- Problem 4
  - Spamtrap vs. Pharmer / phishing malware
  - And the winner is:

- Solution
  - Phoneybot = honeypot as a robot against phishing



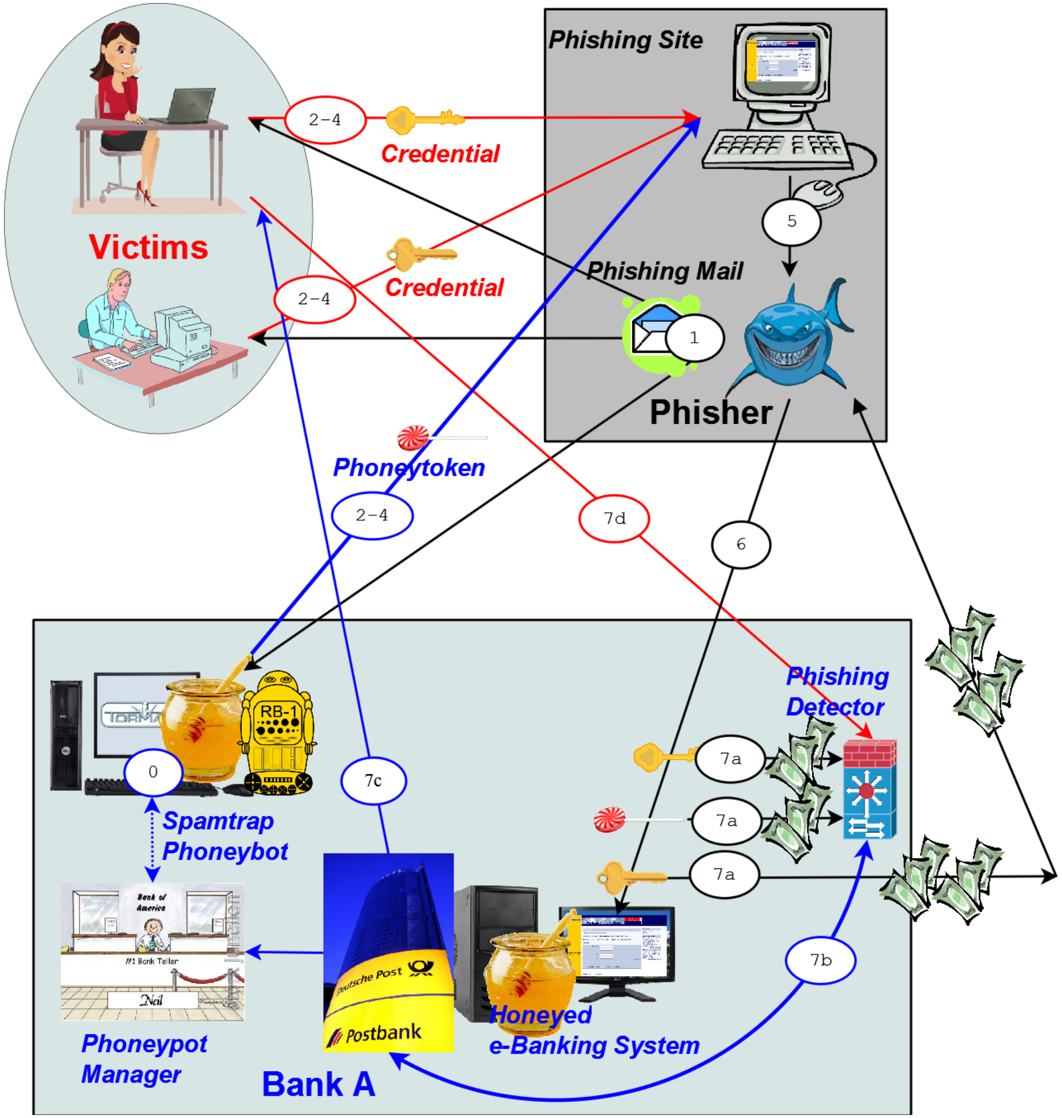
  - Phoneybots @ Virtual machines (NO security protection)
  - Phoneybots ≈ Average users

Anti-Phishing Honeypots: What’s wrong, folks?

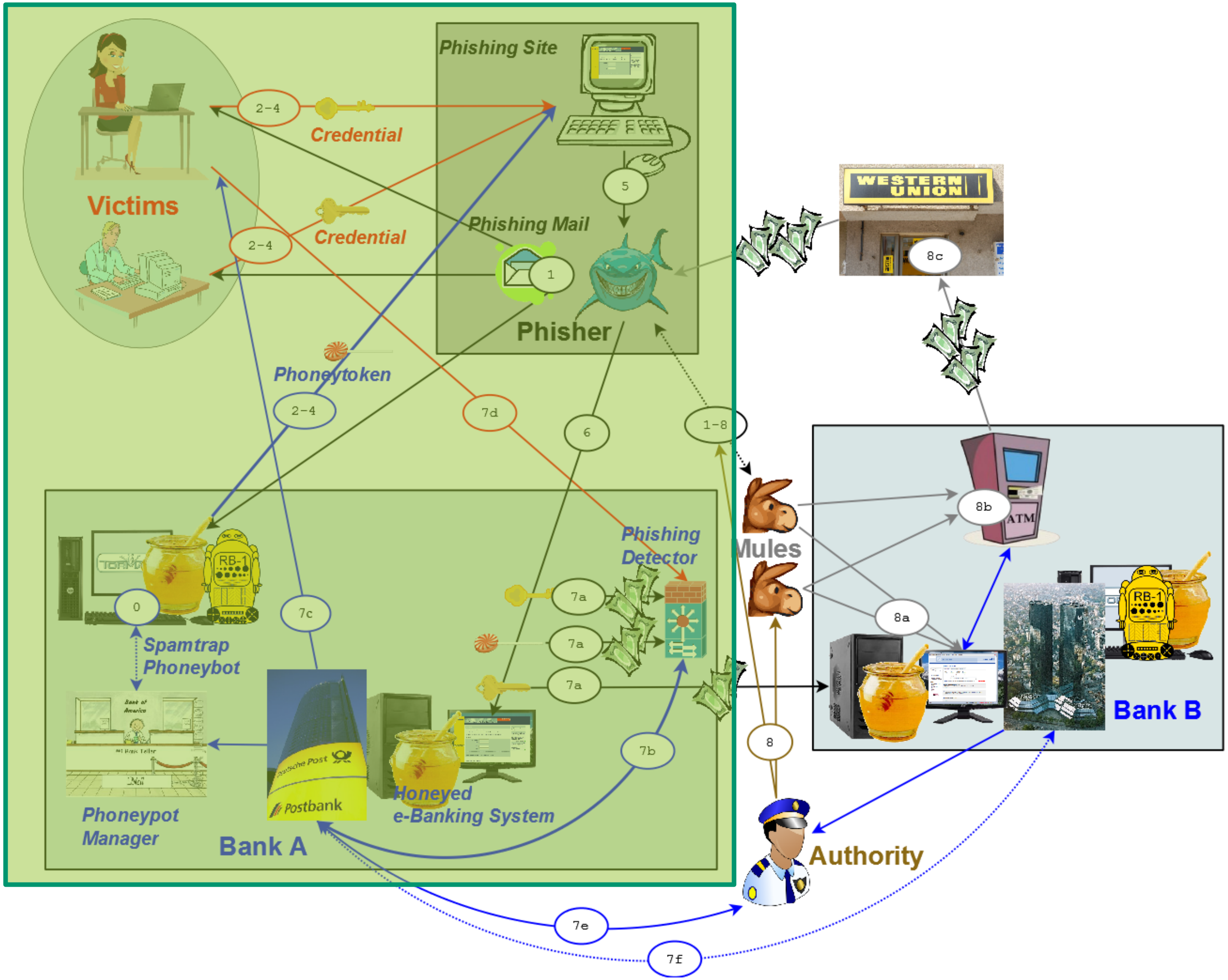
- Problem 5
  - Outsourcing reduces response time
  - Outsourcing causes privacy concerns
  - Outsourcing leads to a higher risk of insider attacks

- Solution
  - Security should NOT be outsourced ⇒
  - The whole anti-phishing chain should be under the control of the financial institute.
  - But, cooperation between different financial institutes and anti-phishing bodies is still very important.

The proposed framework



The proposed framework: Phisher and his mules



The proposed framework: Selected features

- A complete anti-phishing chain established
- Four different kinds of honeypots in one system
- User reconfirmation via out-of-band (OOB) channel
- Phishing detector vs. Phishers
  - No alert if a fund transfer is below a threshold *H*
  - Attacker’s behavior is considered
  - A probabilistic analysis is included
- No requirement/dependence for/on the user
- Devil is in the detail…

Read our paper to find it ☺

Summary, or Take-Home Messages

- Put various kinds of honeypots together ⇒ A new anti-phishing framework
  - Phishers and/or their mules may be detected
  - Victims may be rescued

- Open Questions:
  - Are faster banks worse than slower ones?
  - Will banks be willing to bear additional costs for deploying the framework?
  - How to reduce the additional costs incurred while keeping an acceptably low false positive/negative detection rate?
  - A real implementation is to be done …

Thanks for your attention!

Any questions?

Shujun Li: www.hooklee.com

Roland Schmitz: schmitz@hdm-stuttgart.de

General Members Meeting &
eCrime Researchers Summit
October 19, 20 & 21, 2009 – Tacoma, WA