A Preliminary Scheme for Combating Phishing with Zero Knowledge Authentication

Trust is for Suckers

Paul Knickerbocker
pknicker@cs.uoregon.edu
NetSec Lab - University of Oregon

Advisors: Jun Li (lijun@cs.uoregon.edu), Du Li (lidu008@gmail.com)

The Phishing Problem

What is Phishing

Phishing is a way of getting users to disclose their login information by tricking them into logging-in to a fraudulent website which mimics a legitimate site the user has an account at.

A Typical Phishing Scenario

1. Phisher downloads a copy of legitimate site

2. Phisher duplicates the website and posts it on his own server

3. Phisher sends out emails to website users with a link to the Phisher's fake website

4. Website user tries to log into fake website, sending their **username** and **password**

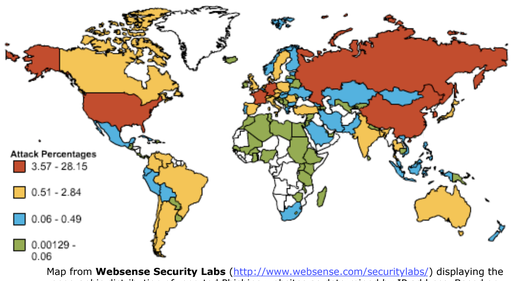
5. Phisher uses the stolen **username** and **password** to log into the legitimate website

** Other techniques (often called **Pharming**) divert users away from their legitimate websites by modifying DNS records.*

Reported Phishing sites - '06 to '07

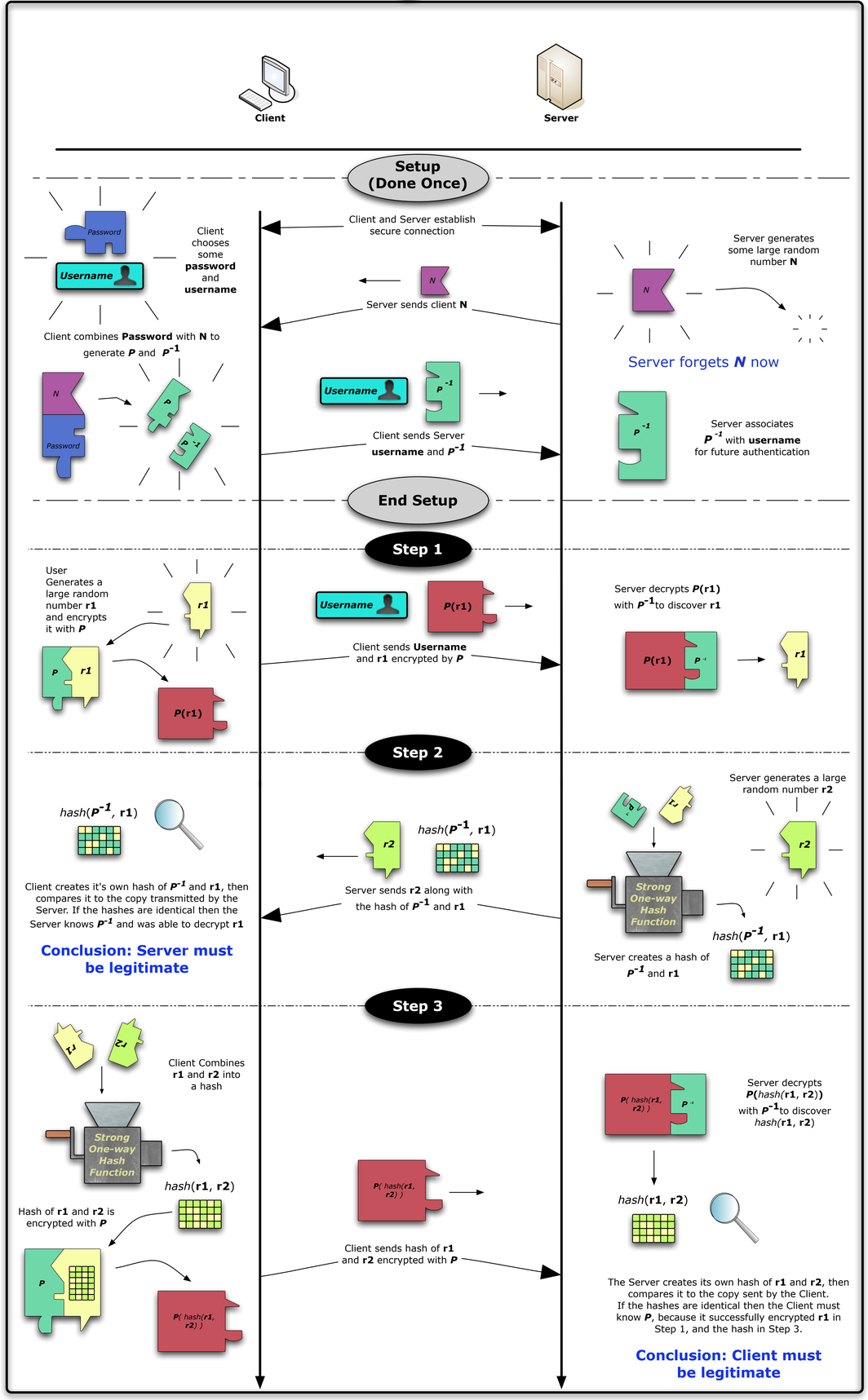
Graph from **The Anti-Phishing Working Group's** (http://www.antiphishing.org) *Attack Trends Report for June '07*

Where Phishing sites come from, by %



Map from **Websense Security Labs** (http://www.websense.com/securitylabs/) displaying the geographic distribution of reported Phishing websites as determined by IP address. Based on data collected from Sep '06 to Sep '07

Our Zero Knowledge Scheme



What is Zero Knowledge?

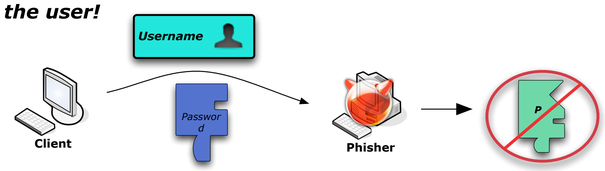
In a Zero Knowledge Password authentication scheme both parties have unique passwords. Each party can confirm that the other party knows its own password, but neither party knows what the other parties password is. We implement Zero Knowledge by using the user's password to create asymmetric keys, like those used in public key cryptography.

Hard Truths We Confront

- Most users are unsophisticated. **Users *will* give their passwords to Phishers**. Our scheme makes Phishing pointless. Usernames and passwords are not enough to access the user's account.
- Software that tries to determine if a website is legitimate by analyzing HTML ***will not* detect every Phishing website**. Site authentication is built into our scheme.

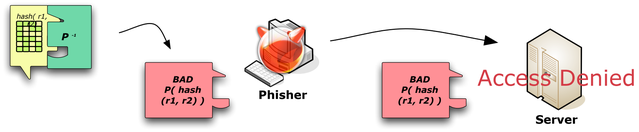
Advantages of our Scheme

Even if a Phisher discovers user name and password they cannot log in as the user!



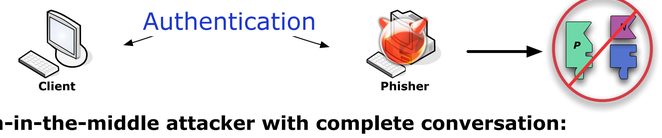
Even if the Phishier steals all the authentication data from the Server:

- The Phisher cannot log in as the user to the legitimate Server (*Step #3*).



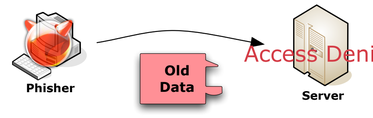
- The Phisher cannot discover the user's ***Password, P*** or ***N***.

- The Phisher can't discover ***P*** or ***N*** by pretending to be the server and authenticating the user.



A Man-in-the-middle attacker with complete conversation:

- cannot replay the authentication.



- won't discover anything about **Password**, **N, r1, P** or **P^{-1}**.