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

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

What is Phishing?

Where Phishing sites come from, by %

Reported Phishing sites - ’06 to ’07

A Preliminary Scheme for Combating Phishing with Zero Knowledge Authentication
Trust is for Suckers

Paul Knickerbocker
pk@cs.uoregon.edu

Advisors: Jiun Li (jil@cs.uoregon.edu), Du Li (lidu008@gmail.com)