

# **L22: Authentication & passwords**

Nickolai Zeldovich  
6.033 Spring 2011

# Password-based authentication

```
checkpw(user, passwd):  
    acct = accounts[user]  
    for i in range(0, len(acct.pw)):  
        if acct.pw[i] ≠ passwd[i]:  
            return False  
    return True
```

# Password hashing

```
checkpw(user, passwd):  
    acct = accounts[user]  
    h = SHA1(passwd)  
    if acct.pwhash ≠ h:  
        return False  
    return True
```

# Password statistics (leaked list of 32M pws, 2009)

## Password Popularity – Top 20

| Rank | Password  | Number of Users with Password (absolute) |
|------|-----------|--|
| 1    | 123456    | 290731                                   |
| 2    | 12345     | 79078                                    |
| 3    | 123456789 | 76790                                    |
| 4    | Password  | 61958                                    |
| 5    | iloveyou  | 51622                                    |
| 6    | princess  | 35231                                    |
| 7    | rockyou   | 22588                                    |
| 8    | 1234567   | 21726                                    |
| 9    | 12345678  | 20553                                    |
| 10   | abc123    | 17542                                    |

| Rank | Password | Number of Users with Password (absolute) |
|------|----------|--|
| 11   | Nicole   | 17168                                    |
| 12   | Daniel   | 16409                                    |
| 13   | babygirl | 16094                                    |
| 14   | monkey   | 15294                                    |
| 15   | Jessica  | 15162                                    |
| 16   | Lovely   | 14950                                    |
| 17   | michael  | 14898                                    |
| 18   | Ashley   | 14329                                    |
| 19   | 654321   | 13984                                    |
| 20   | Qwerty   | 13856                                    |

- 5,000 unique passwords account for 20% of users (6.4 million)
- Similar statistics confirmed again in 2010 (Gawker break-in)

# Password hashing with salt

```
checkpw(user, passwd):  
    acct = accounts[user]  
    h = SHA1(acct.pwsalt + passwd)  
    if acct.pwhash ≠ h:  
        return False  
    return True
```

# “Sitekey”

The screenshot shows a web browser window with the following elements:

- Browser Tab:** Home Banking
- Address Bar:** <https://global1.onlinebank.com/vtg/preauthenticatereuser.htm?loginUrl=4D4E35D99687A9327764>
- Page Header:** Print | Help
- Section Header:** Log In to Your Account
- CAPTCHA:** A square image of a bear's head with the text "not an elephant" below it.
- Text:** Please Enter Your Password Only After Verifying Your Personal Image.
- Form Fields:** User ID : zeldovich1, Password :
- Links:** [Forgot your Password?](#)
- Buttons:** Back, Login
- Logos:** VeriSign Trusted logo with the text "VERIFY" below it.