6.033 Computer System Engineering

Spring 2009

6.033 Lecture 21
Security Introduction

Nickolai Zeldovich

Security is a big problem

- 250M people's private data stolen in last 4 yrs
- 50% of web servers vulnerable to some attack
- Over 20 new security bugs found *every day*
  - 1 critical Windows security problem a week, on avg

paymaxx.com: online tax forms

- https://my.paymaxx.com/
  - Requires username and password
  - If you authenticate, provides menu of options
  - One option is to get a PDF of your W2 tax form

** URLs simplified for presentation*

paymaxx.com: online tax forms

- https://my.paymaxx.com/
  - Requires username and password
  - If you authenticate, provides menu of options
  - One option is to get a PDF of your W2 tax form
- https://my.paymaxx.com/get-w2.cgi?id=1234
  - Gets a PDF of W2 tax form for ID 1234

** URLs simplified for presentation*

paymaxx.com: online tax forms

- https://my.paymaxx.com/
  - Requires username and password
  - If you authenticate, provides menu of options
  - One option is to get a PDF of your W2 tax form
- https://my.paymaxx.com/get-w2.cgi?id=1234
  - Gets a PDF of W2 tax form for ID 1234
- get-w2.cgi forgot to check authorization
  - Attacker manually constructs URLs to fetch all data

** URLs simplified for presentation*

Security and naming

```
athena% cd ~bob/project
athena% cat ideas.txt
Our plan is to build a more secure OS,
by providing flexible authentication
and authorization mechanisms.
...
athena%
```

Security and naming

```
athena% cd ~bob/project
athena% cat ideas.txt
Our plan is to build a more secure OS,
by providing flexible authentication
and authorization mechanisms.
...
athena% < ideas.txt
athena%
```

Security and naming

```
athena% cd ~bob/project
athena% cat ideas.txt
Our plan is to build a mor
by providing flexible auth
and authorization
...
athena% < ideas.txt
athena%
```

Bob changes ideas.txt to a symbolic link to 6.033's grades.txt

Password-based authentication

```
bool checkpw(string username, string password):

    string knownpw = userdb.lookup(username)

    if (knownpw.len != password.len):
        return FALSE

    for (i: 0 .. password.len-1):
        if (knownpw[i] != password[i]):
            return FALSE

    return TRUE
```