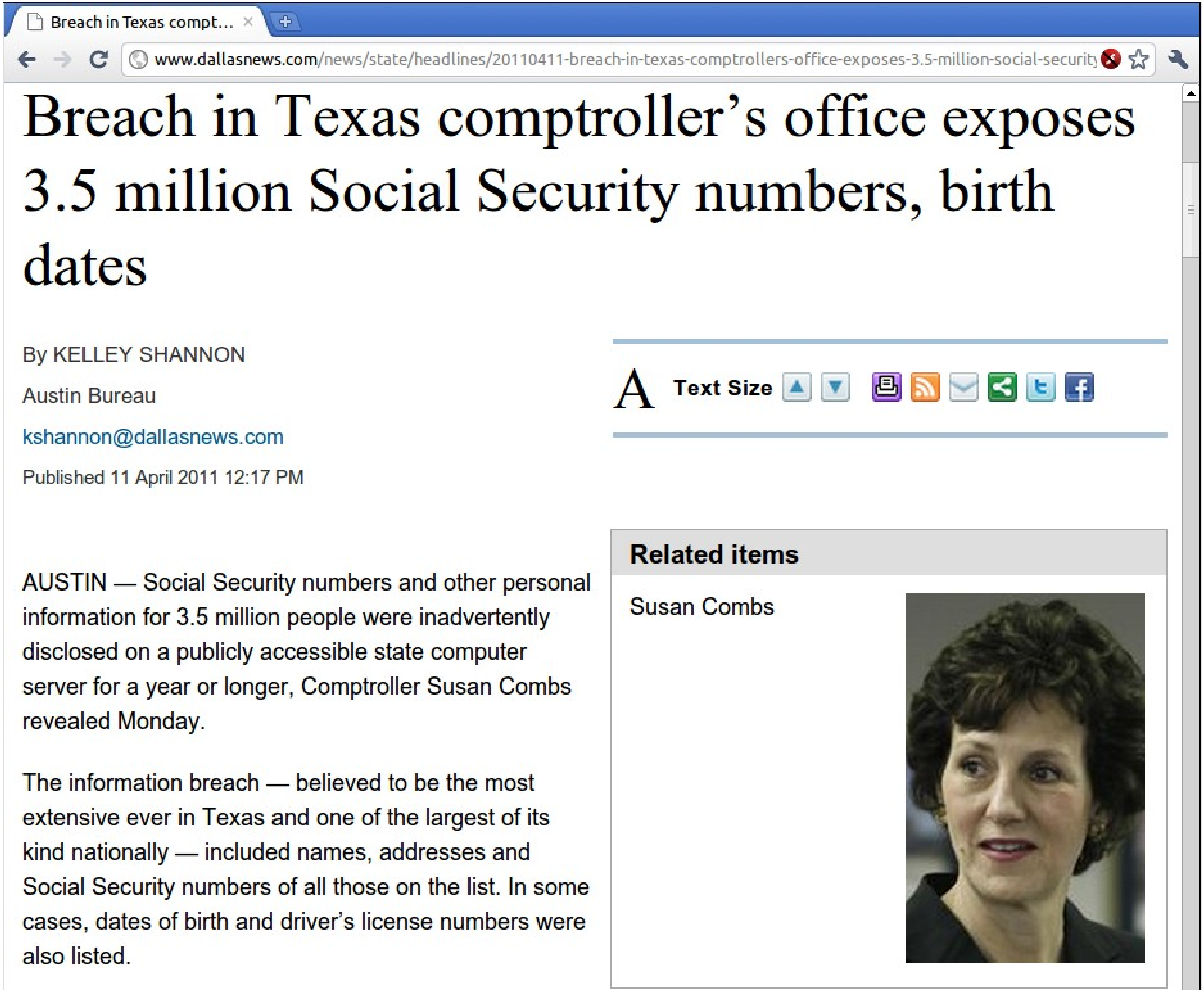
L21: Security intro

Nickolai Zeldovich
6.033 Spring 2011

Private data routinely leaked


Breach in Texas compt...
www.dallasnews.com/news/state/headlines/20110411-breach-in-texas-comptrollers-office-exposes-3.5-million-social-security
A Text Size

Breach in Texas comptroller’s office exposes 3.5 million Social Security numbers, birth dates

By KELLEY SHANNON
Austin Bureau
kshannon@dallasnews.com
Published 11 April 2011 12:17 PM

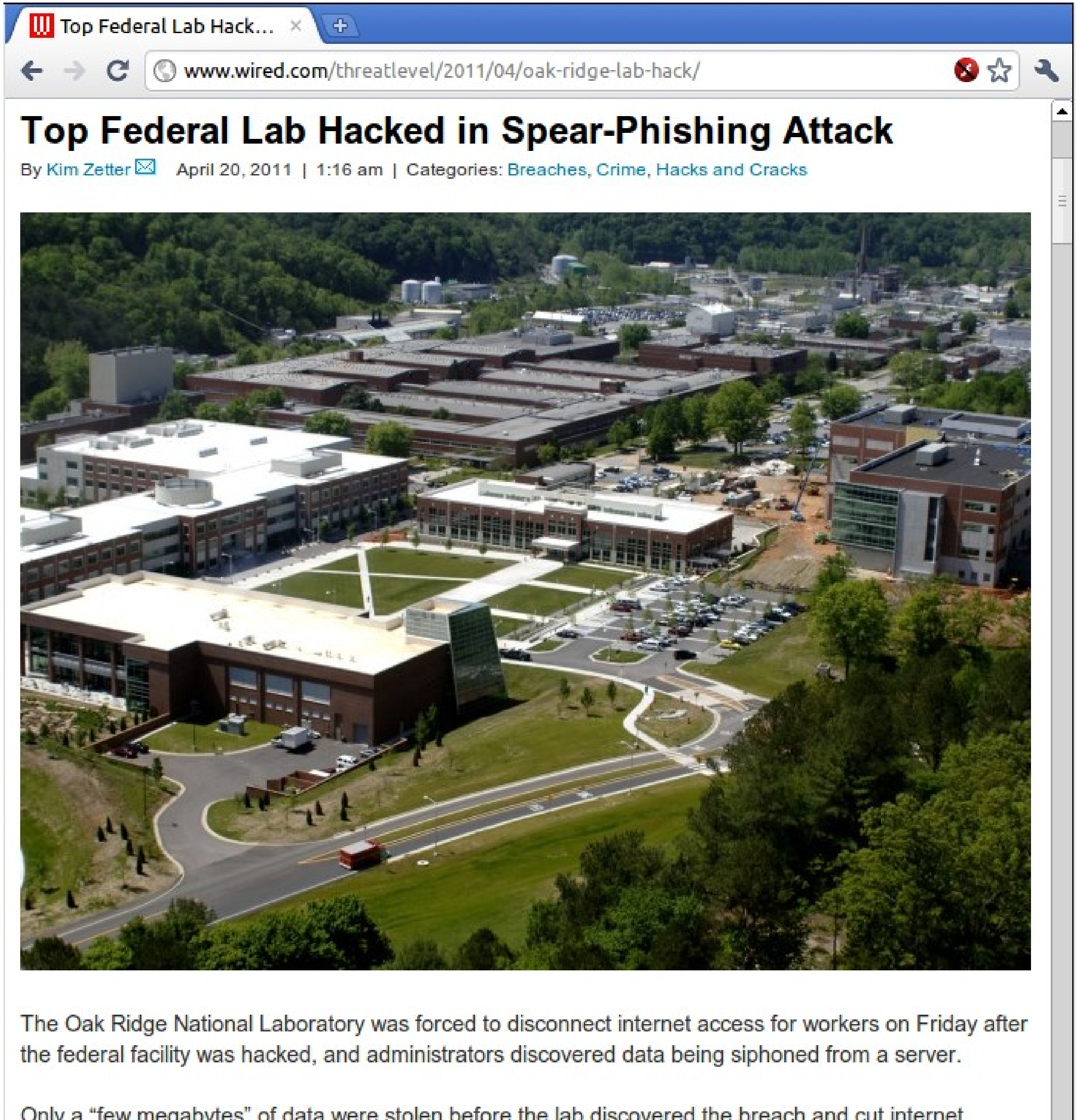
AUSTIN — Social Security numbers and other personal information for 3.5 million people were inadvertently disclosed on a publicly accessible state computer server for a year or longer, Comptroller Susan Combs revealed Monday.

The information breach — believed to be the most extensive ever in Texas and one of the largest of its kind nationally — included names, addresses and Social Security numbers of all those on the list. In some cases, dates of birth and driver’s license numbers were also listed.

Related items

Susan Combs

Users tricked by impersonators



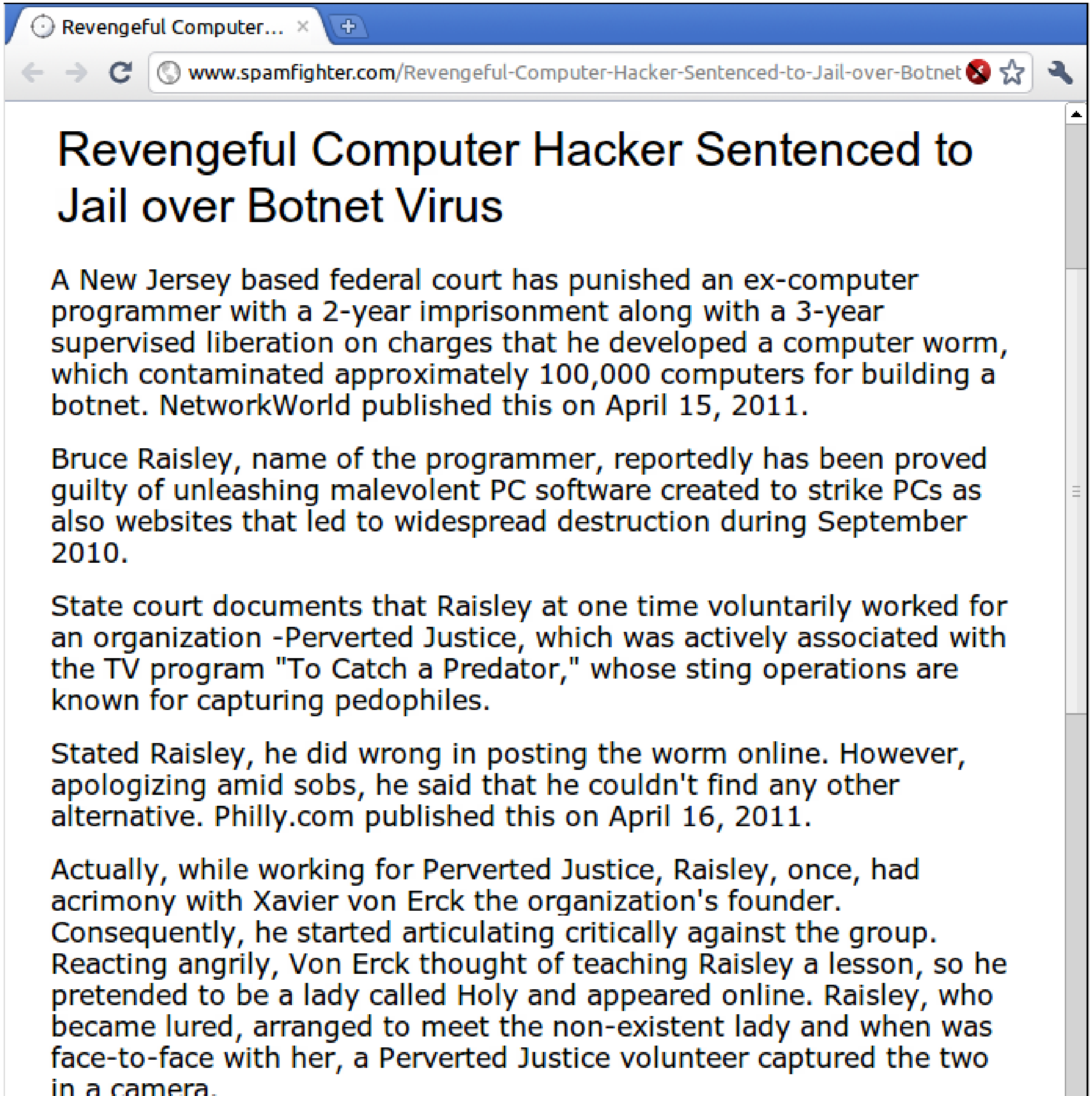
Top Federal Lab Hacked in Spear-Phishing Attack

By Kim Zetter April 20, 2011 | 1:16 am | Categories: Breaches, Crime, Hacks and Cracks

The Oak Ridge National Laboratory was forced to disconnect internet access for workers on Friday after the federal facility was hacked, and administrators discovered data being siphoned from a server.

Only a “few megabytes” of data were stolen before the lab discovered the breach and cut internet

Botnets control millions of PCs



Revengeful Computer...
www.spamfighter.com/Revengeful-Computer-Hacker-Sentenced-to-Jail-over-Botnet

Revengeful Computer Hacker Sentenced to Jail over Botnet Virus

A New Jersey based federal court has punished an ex-computer programmer with a 2-year imprisonment along with a 3-year supervised liberation on charges that he developed a computer worm, which contaminated approximately 100,000 computers for building a botnet. NetworkWorld published this on April 15, 2011.

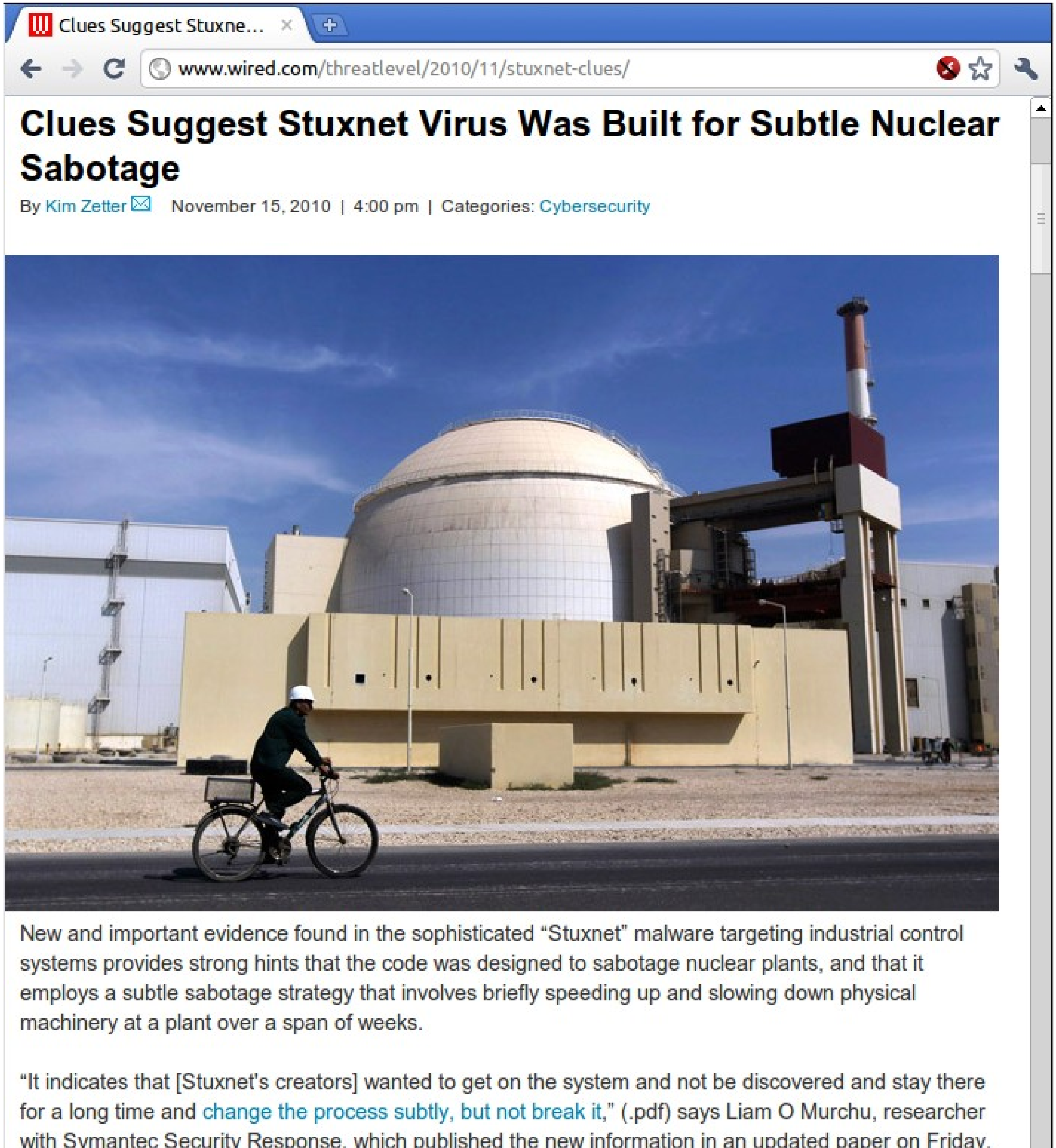
Bruce Raisley, name of the programmer, reportedly has been proved guilty of unleashing malevolent PC software created to strike PCs as also websites that led to widespread destruction during September 2010.

State court documents that Raisley at one time voluntarily worked for an organization -Perverted Justice, which was actively associated with the TV program "To Catch a Predator," whose sting operations are known for capturing pedophiles.

Stated Raisley, he did wrong in posting the worm online. However, apologizing amid sobs, he said that he couldn't find any other alternative. Philly.com published this on April 16, 2011.

Actually, while working for Perverted Justice, Raisley, once, had acrimony with Xavier von Erck the organization's founder. Consequently, he started articulating critically against the group. Reacting angrily, Von Erck thought of teaching Raisley a lesson, so he pretended to be a lady called Holy and appeared online. Raisley, who became lured, arranged to meet the non-existent lady and when was face-to-face with her, a Perverted Justice volunteer captured the two in a camera.

Computer worm used to sabotage



Clues Suggest Stuxnet Virus Was Built for Subtle Nuclear Sabotage

By Kim Zetter November 15, 2010 | 4:00 pm | Categories: Cybersecurity

New and important evidence found in the sophisticated "Stuxnet" malware targeting industrial control systems provides strong hints that the code was designed to sabotage nuclear plants, and that it employs a subtle sabotage strategy that involves briefly speeding up and slowing down physical machinery at a plant over a span of weeks.

"It indicates that [Stuxnet's creators] wanted to get on the system and not be discovered and stay there for a long time and change the process subtly, but not break it," (.pdf) says Liam O Murchu, researcher with Symantec Security Response, which published the new information in an updated paper on Friday.

paymaxx.com (2005)

- 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

* simplified URLs

paymaxx.com (2005)

- 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

* simplified URLs

paymaxx.com (2005)

- 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

* simplified URLs

Layer interactions: naming

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

Layer interactions: naming

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

Layer interactions: naming

```
athena% cd /mit/bob/project
athena% cat ideas.txt
Our plan is to build a more se
by providing flexible authenti
and authorization mechan
...
athena% mail chuck@mit.edu < ideas.txt
athena%
```

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