6.033 Lecture 21
Security Introduction

Nickolai Zeldovich

Spring 2009

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

The New York Times

March 29, 2009

Vast Spy System Loots Computers in 103 Countries

By JOHN MARKOFF

TORONTO — A vast electronic spying operation has infiltrated computers and has stolen documents from hundreds of government and private offices around the world, including those of the Dalai Lama, Canadian researchers have concluded.

In a report to be issued this weekend, the researchers said that the system was being controlled from computers based almost exclusively in China, but that they could not say conclusively that the Chinese government was involved.

The researchers, who are based at the Munk Center for International Studies at the University of Toronto, had been asked by the office of the Dalai Lama, the exiled Tibetan leader whom China regularly denounces, to examine its computers for signs of malicious software, or malware.

Their sleuthing opened a window into a broader operation that, in less than two years, has infiltrated at least 1,295 computers in 103 countries, including many belonging to embassies, foreign ministries and other government offices, as well as the Dalai Lama's Tibetan exile centers in India, Brussels, London and New York.

The researchers, who have a record of detecting computer espionage, said they believed that in addition to the spying on the Dalai Lama, the system, which they called GhostNet, was focused on the governments of South Asian and Southeast Asian countries.

Intelligence analysts say many governments, including those of China, Russia and the United States, and other parties use sophisticated computer programs to covertly gather information.

The New York Times
nytimes.com

March 12, 2008

A Heart Device Is Found Vulnerable to Hacker Attacks

By BARNABY J. FEDER

To the long list of objects vulnerable to attack by computer hackers, add the human heart.

The threat seems largely theoretical. But a team of computer security researchers plans to report Wednesday that it had been able to gain wireless access to a combination heart defibrillator and pacemaker.

They were able to reprogram it to shut down and to deliver jolts of electricity that would potentially be fatal — if the device had been in a person. In this case, the researcher were hacking into a device in a laboratory.

The researchers said they had also been able to glean personal patient data by eavesdropping on signals from the tiny wireless radio that Medtronic, the device's maker, had embedded in the implant as a way to let doctors monitor and adjust it without surgery.

The report, to published at www.secure-medicine.org, makes clear that the hundreds of thousands of people in this country with implanted defibrillators or pacemakers to regulate their damaged hearts — they include Vice President Dick Cheney — have no need yet to fear hackers. The experiment required more than $30,000 worth of lab equipment and a sustained effort by a team of specialists from the University of Washington and the University of Massachusetts to interpret the data gathered from the implant's signals. And the device the researchers tested, a combination defibrillator and pacemaker called the Maximo, was placed within two inches of the test gear.

Defibrillators shock hearts that are beating chaotically and dangerously back into normal rhythms. Pacemakers use gentle stimulation to slow or speed up the heart. Federal regulators said no security breaches of such medical implants had ever been reported to them.

Click here to print

Mail Online

Prisoner wrongly freed after officials get phony, typo-filled fax from grocery store

Last updated at 10:17 23 April 2007

Officials mistakenly released a prisoner from a Kentucky facility after receiving a phony fax that ordered him freed, and it took them nearly two weeks to realize it.

The fax contained grammatical errors, was not typed on letterhead and was sent from a local grocery store. The fax falsely claimed that the Kentucky Supreme Court "demanded" Timothy Rouse be released.

Rouse, 19, is charged with beating an elderly man and was at the Kentucky Correctional & Psychiatric Center in La Grange for a mental evaluation. He was released April 6 after officials received the fake court order.

Lexington police arrested Rouse at his mother's home Thursday evening.

"It's outrageous that it happened," Fulton County Attorney Rick Major said. "I'm just glad nobody got hurt because he's dangerous."

Police are still investigating who faxed the letter.

Attorney Carlos Moran, who is representing Rouse, declined to comment.

Prison officials did not notice that the fax came from the grocery store because policies did not require checking the source of a faxed order, said the LaGrange facility's director, Greg Taylor.

"It's not part of a routine check, but certainly, in hindsight, that would perhaps have caused somebody to ask a question," he said.

Misspellings on orders are common, he said.

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% mail chuck@mit.edu < 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 me
...
athena% mail chuck@mit.edu < 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
```