Advanced Computer Security

Fall 2012

Martín Abadi

University of California, Santa Cruz

Instructor information

Instructor: Martín Abadi

- Office: E2 347A
- Email: abadi@cs.ucsc.edu
- Web: www.soe.ucsc.edu/~abadi/home.html
- Office hours: Tuesdays and Thursdays before class, 9am to 9:45am.

Instructor information (cont.)

Research in:

- computer and network security,
- programming languages,
- specification and verification methods.

Course web pages

www.soe.ucsc.edu/~abadi/CS223_F12/home.html

Student information

Please write down:

- name,
- email address,
- program (e.g., MS in CS),
- year of study.

Please display your name in front of you
(at least for a couple of weeks).

Prerequisites

Some familiarity with computer systems:

- operating systems,
- networks,
- programming languages.

Some mathematical sophistication:

- a little number theory,
- ability to follow and do proofs, e.g., by induction,
- acquaintance with mathematical logic,
- ease with formal notation and manipulation,

but no advanced mathematics required.

Prerequisites (cont.)

Please see me if you are

- not sure that you meet the prerequisites, or
- an undergraduate, or
- a graduate student from outside CS or CE.

Contents

- A graduate-level course.
- An introduction to basic concepts and techniques in computer and network security.
- A look at some more advanced topics.

Main course topics

- Basics and principles.
- Access control (including ACLs, capabilities, …).
- Information-flow control.
- Security in programming languages.
- Low-level software security.
- Cryptography.
- Security of basic network protocols and services.
- PKIs.
- Security protocols (such as SSL).
- User authentication.
- Protocol analysis.

Likely guests

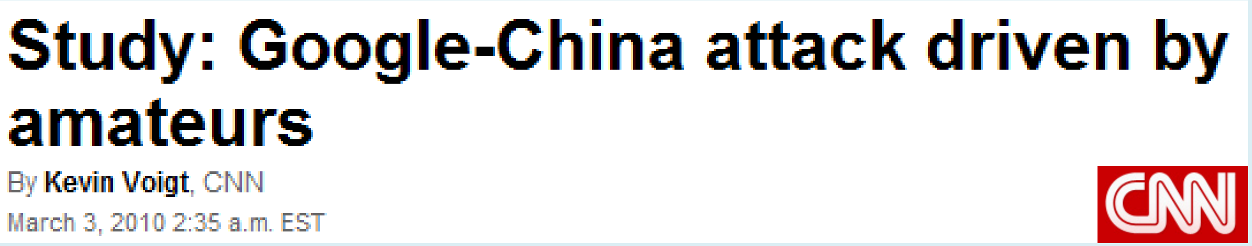
- Frank McSherry (Microsoft)
- Ulfar Erlingsson (Google)
- Ankur Taly (Google)
- Omer Reingold (Microsoft)

The many facets of security

The study of security intersects with many domains:

- cryptography,
- mathematics,
- operating systems,
- networking,
- human-computer interaction,
- economics,
- policy and law.

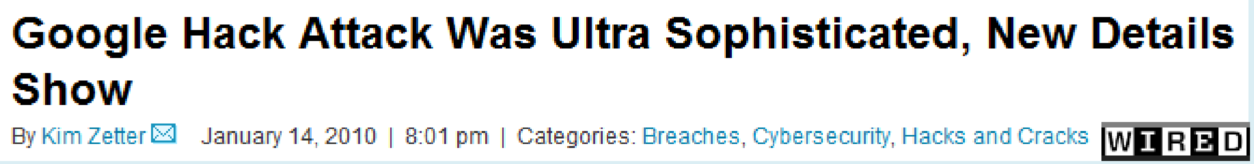
We should at least touch on all of these, but will not even attempt to cover all aspects of the subject.



Study: Google-China attack driven by amateurs

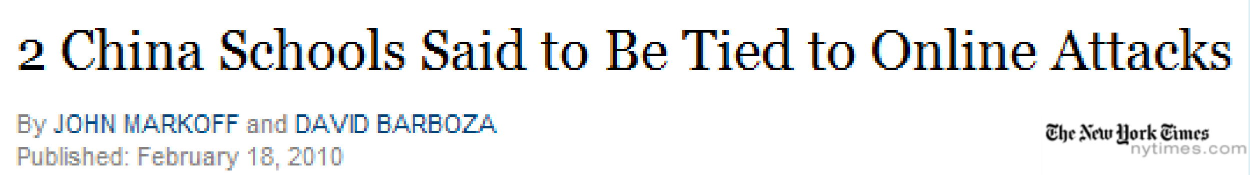
By **Kevin Voigt**, CNN

March 3, 2010 2:35 a.m. EST



Google Hack Attack Was Ultra Sophisticated, New Details Show

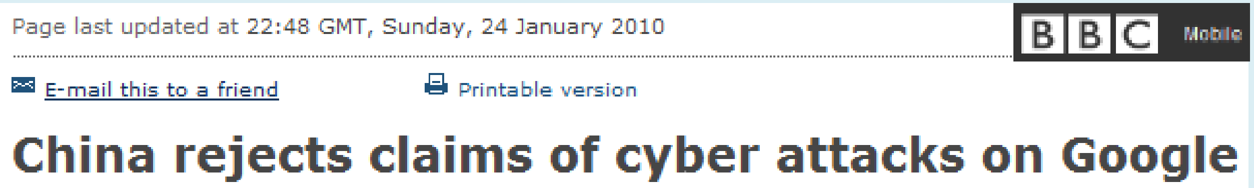
By Kim Zetter ✉ January 14, 2010 | 8:01 pm | Categories: Breaches, Cybersecurity, Hacks and Cracks



2 China Schools Said to Be Tied to Online Attacks

By JOHN MARKOFF and DAVID BARBOZA

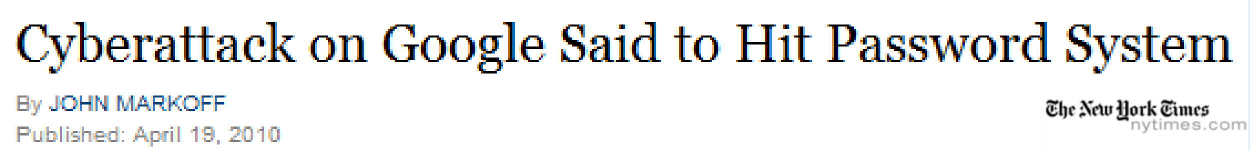
Published: February 18, 2010



Page last updated at 22:48 GMT, Sunday, 24 January 2010

✉ E-mail this to a friend 🖶 Printable version

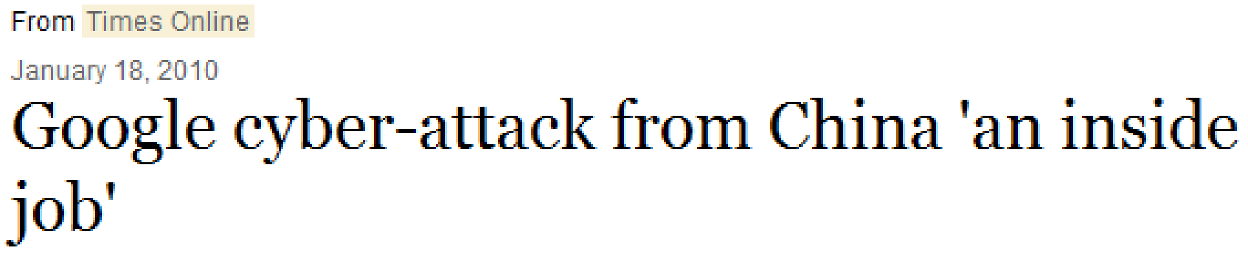
China rejects claims of cyber attacks on Google



Cyberattack on Google Said to Hit Password System

By JOHN MARKOFF

Published: April 19, 2010



From Times Online

January 18, 2010

Google cyber-attack from China 'an inside job'

There are known knowns: there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns: the ones we don't know we don't know.

Rumsfeld

Reading

Required reading:

- No textbook!
- Various papers, indicated during the course.

Some recommended reading:

- Ross Anderson's book: *Security engineering: A guide to building dependable distributed systems* www.cl.cam.ac.uk/~rja14/book.html
- For background on classic cryptography, *The handbook of applied cryptography* www.cacr.math.uwaterloo.ca/hac/index.html

More reading

- Schneier’s *Secrets and lies*,
- Mitnick’s *The art of deception*,
- Bishop’s *Computer Security: Art and Science*,
- Ferguson et al.’s *Cryptography Engineering*,
- Milner’s *Communicating and mobile systems: the π -calculus*,
- Zalewski’s *The Tangled Web* easyride.quaxio.com/Tangled_Web.pdf.

Other resources

- Web sites and mailing lists with reports of incidents, e.g., www.cert.org and www.theregister.co.uk/security/.
- Conferences:
  - Crypto and Eurocrypt,
  - IEEE Symposium on Security and Privacy,
  - ACM Conference on Computer and Communications Security,
  - Usenix Security Symposium,
  - Network and Distributed System Security Symposium,
  - IEEE Computer Security Foundations Symposium,
  - occasionally conferences in other areas (SOSP, POPL, WWW, ….),
  - blackhat, defcon, etc..

Course work

- Reading.
- Class participation.
- Homework:
  - announced and explained in class,
  - posted as part of the slides or with the slides,
  - often due at the start of class one week later (strictly!),
  - mostly but not always fairly easy,
  - sometimes with class presentation or discussion.
- A medium-size final project.
- No exams.

The final project

Several kinds (to be described in a moment), all with brief reports.

Surveys must be done by one person.

Other projects may be done by teams of appropriate size (up to 4).

Collaboration

You can do the projects (except for surveys) in groups of 1–4.

If you have a great project idea, and it looks too big for one person, feel free to recruit help.

I think that it is easier to do the projects alone, but you are welcome to make your own choices.

Picking a project

You are encouraged to define your own project.

If you prefer it, I will be happy to assign you a project, but I can’t guarantee that you will be happy with it.

Scale

I don’t expect very fancy projects.

30–40 hours of work should suffice, unless you are very enthusiastic.

If you decide to tackle a more ambitious project, you should structure it so that you can show at least partial results this quarter.

Kinds of projects

There are three basic kinds of projects:

- Survey of work in some area of security.
- Implementation of some security mechanism.
- Research in security.

These kinds can be combined to some extent.

In all cases, you must write a short report and make a short presentation.

The survey project

Pick an area in which you may be interested. For example:

- information-flow control in browsers,
- search-engine abuse,
- some particular kind of security protocols (e.g., metering, password-based authentication),
- verification tools for protocols,
- security of some particular sort of systems (e.g., storage systems, hospitals),
- block ciphers and their modes of operations.

For more ideas, see the proceedings of recent conferences.

The survey project (cont.)

Read well 2–5 papers (or a monograph?).

Read at least superficially 2–5 extra papers.

Write a short report on what you have learned.

- What are the basic problems in this area?
- What are the basic approaches to solving them?
- What are the main achievements to date?

Keep the project narrow enough that you can say something interesting!

The implementation project

Implement some (non-trivial) security mechanism. For example:

- a little protocol,
- some static program analysis related to security,
- an auditing tool.

This sort of project is most appropriate in the context of a larger system that you are developing.

Write a short report on your project (1–2 pages).

How much code? There is no firm limit.

- 50 lines is probably too small.
- 5,000 is probably too big.

The research project

There are many sorts of research projects:

- Develop new security policies, mechanisms, and assurance techniques.
- Try to apply existing ones in new settings.
- Evaluate defenses.
- Develop theories or apply them.
- Explore interesting vulnerabilities.

In all cases, write a report on this work, of whatever length is appropriate.

The writing need not be publication-quality, but I should be able to read it easily.

The research project (cont.)

Research projects are the hardest.

Starting on a survey project and turning it into a research project may be possible, and is recommended unless you have clear research ideas already.

Reports and presentations

Project reports are due on December 4.

We will have brief presentations in class at the end of the quarter. (Please stay tuned.)

Extra work afterwards will be considered only in truly exceptional circumstances.

Grades

Grades are determined as follows:

- project (including its presentation): 45 - 50 %
- homework (and its discussion): 45 - 50 %
- class participation: the rest

Regular class attendance is expected.

Cheating

- All work you turn in must be your own.
- If you don’t know whether something is allowed, please ask.
- Any cheating will result in failure of the course and other standard measures.

Cheating (cont.)

- You are encouraged to discuss the course material and assignments with others.
- You are not allowed to do assignments with others (except projects, with permission).
- You may use any conversations, texts, or other material, as long as you cite your sources.

Cheating (cont.)

Projects should be new and original:

- not a cut-and-paste of prior work (particularly not prior surveys),
- not also fulfilling the requirements of another course (except by special arrangement),
- not something you have already finished.

But it is good if you care about the project beyond completion of this course.

In a group project, you are expected to do your share, and you should notify me if others are not doing theirs.