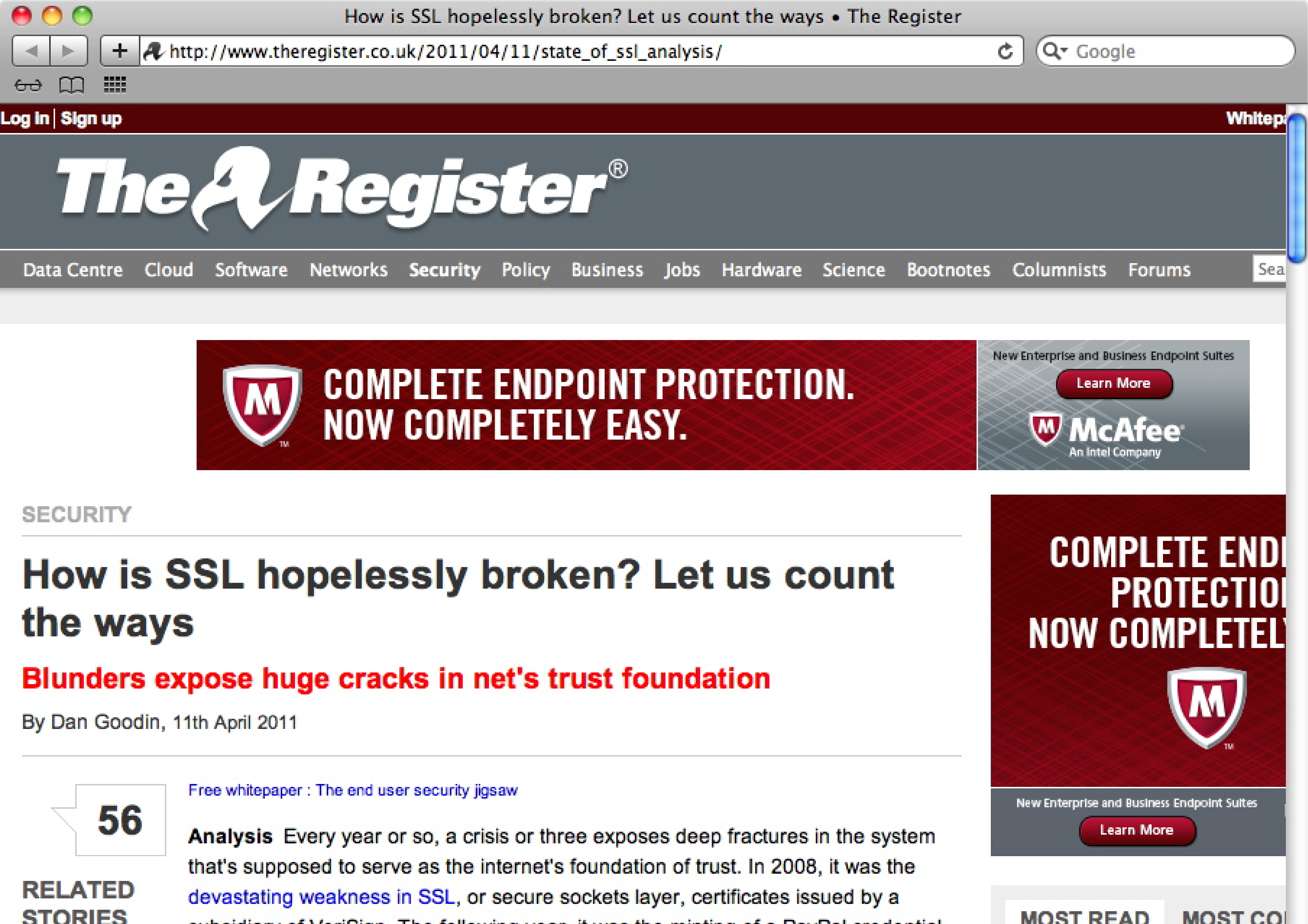
# CS4614 Introductory Network Security

Simon Foley,
(WGB, Room G-65)
Department of Computer Science,
University College Cork
s.foley@cs.ucc.ie

September 7, 2015



SECURITY

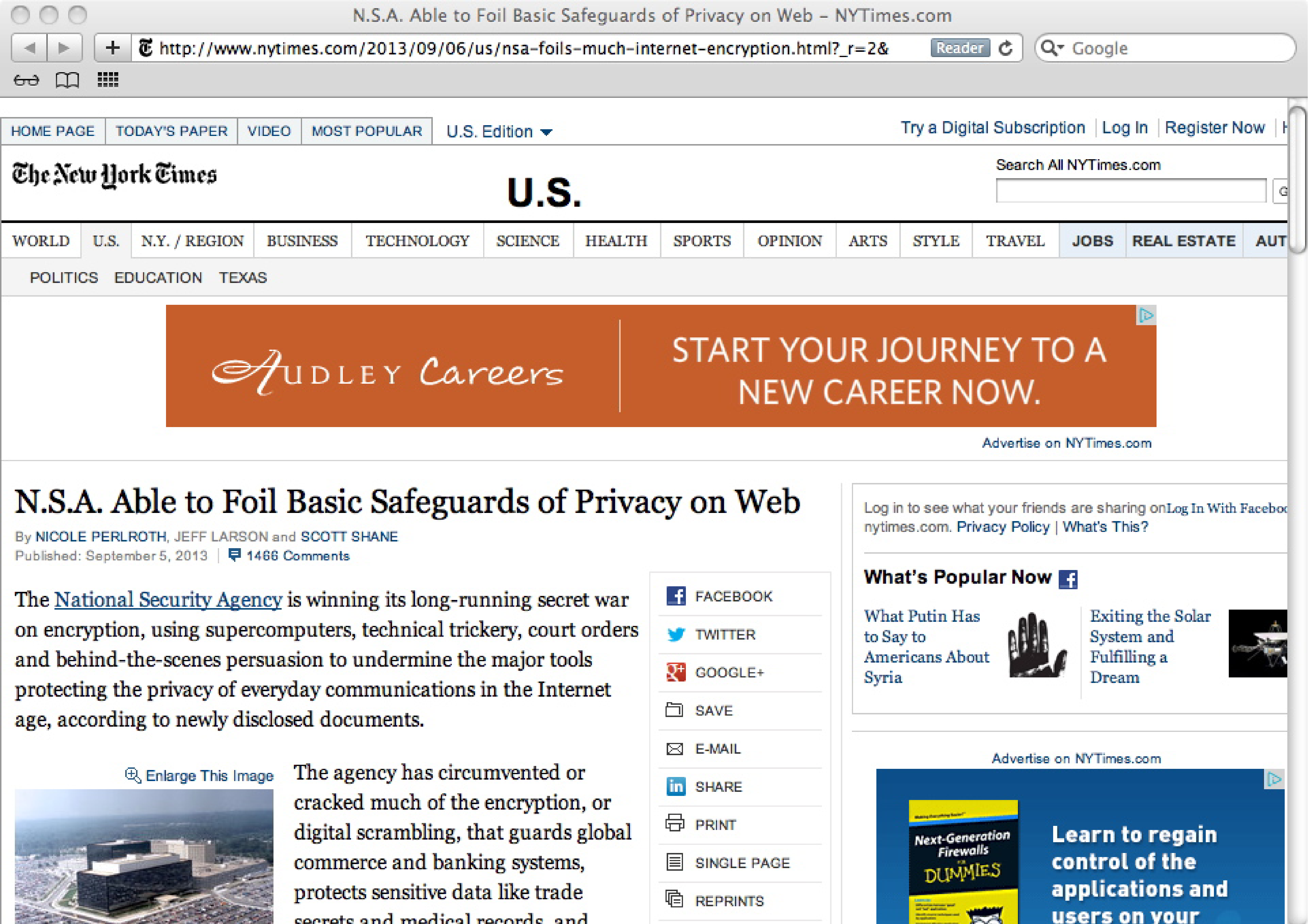
# How is SSL hopelessly broken? Let us count the ways

## Blunders expose huge cracks in net's trust foundation

By Dan Goodin, 11th April 2011

Free whitepaper : The end user security jigsaw

**Analysis** Every year or so, a crisis or three exposes deep fractures in the system that's supposed to serve as the internet's foundation of trust. In 2008, it was the devastating weakness in SSL, or secure sockets layer, certificates issued by a



N.S.A. Able to Foil Basic Safeguards of Privacy on Web – NYTimes.com
http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?_r=2&
Reader
Google
HOME PAGE
TODAY'S PAPER
VIDEO
MOST POPULAR
U.S. Edition
Try a Digital Subscription
Log In
Register Now

The New York Times

U.S.

# N.S.A. Able to Foil Basic Safeguards of Privacy on Web

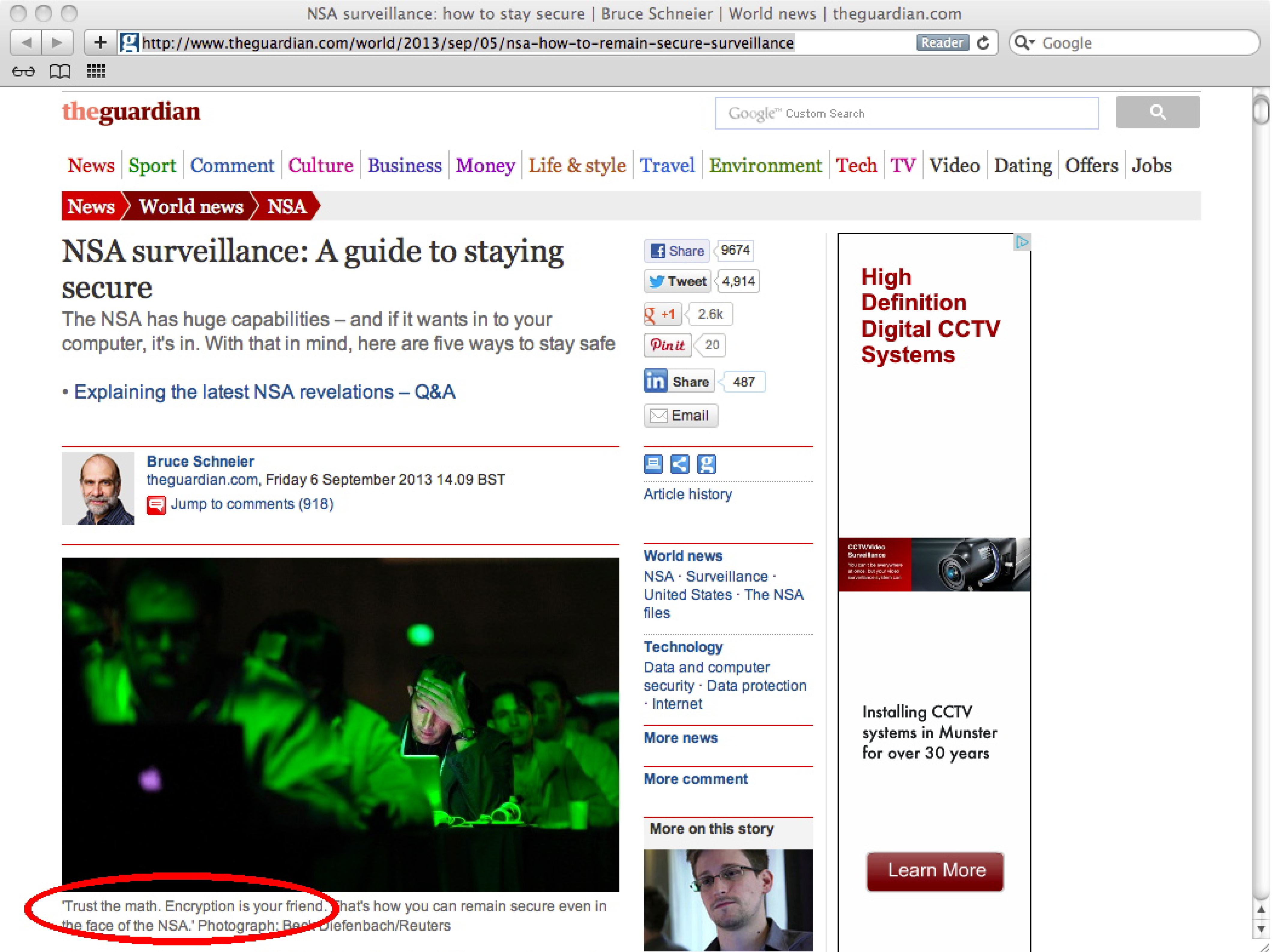
By NICOLE PERLROTH, JEFF LARSON and SCOTT SHANE

Published: September 5, 2013 | 1466 Comments

The National Security Agency is winning its long-running secret war on encryption, using supercomputers, technical trickery, court orders and behind-the-scenes persuasion to undermine the major tools protecting the privacy of everyday communications in the Internet age, according to newly disclosed documents.

The agency has circumvented or cracked much of the encryption, or digital scrambling, that guards global commerce and banking systems, protects sensitive data like trade

Log in to see what your friends are sharing on nytimes.com. Privacy Policy | What's This?
Log In With Facebo
What's Popular Now
What Putin Has to Say to Americans About Syria
Exiting the Solar System and Fulfilling a Dream



NSA surveillance: how to stay secure | Bruce Schneier | World news | theguardian.com

http://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance

# NSA surveillance: A guide to staying secure

The NSA has huge capabilities – and if it wants in to your computer, it's in. With that in mind, here are five ways to stay safe

- Explaining the latest NSA revelations – Q&A

Bruce Schneier
theguardian.com, Friday 6 September 2013 14.09 BST

Jump to comments (918)

'Trust the math. Encryption is your friend.' That's how you can remain secure even in the face of the NSA.' Photograph: Beck Diefenbach/Reuters

Share 9674
Tweet 4,914
+1 2.6k
Pin it 20
Share 487
Email

Article history

World news
NSA · Surveillance · United States · The NSA files

Technology
Data and computer security · Data protection · Internet

More news

More comment

More on this story

# Formalities

# Syllabus

## Semester 1

Introduction to Ciphers. Symmetric key cryptography. Authentication, Secrecy and Integrity. Cryptographic Hash functions and their application. Implementation issues and Cryptographic APIs. Identification Techniques. Authentication and Key Exchange Protocols and their implementation. Design analysis and attacks on security protocols. Public Key Certificates and infrastructure. Digital Signatures. Public Key Infrastructures.

## Learning Outcomes

On successful completion of this module students should be able to:

□ Apply cryptography in the development of basic secure networked systems;

□ analyze and design elementary cryptographic authentication protocols;

□ use cryptographic APIs to provide confidentiality, integrity and authentication across networked application systems.

□ compromise network systems by exploiting common vulnerabilities;

It is important to see how attacks are carried out so as to understand security defenses. However, you must not try these attacks in practice as you will violate the UCC AUP (and most likely the law).

# Prerequisites

Since we'll be using crypto APIs, CS2500 (Java) is a prerequisite (there will be crypto programming assignments).

It is also assumed that you have an understanding of computer systems, computer networking, elementary mathematics, application development and the usual CS problem solving skills.

# Recommended Material/Textbooks

Notes will be provided in class; it is the students responsibility to augment these with *their own notes* of all material covered in class and tutorials. There are a number of good textbooks available and these can provide a second opinion and more in-depth coverage of material discussed in lectures.

Useful books for the course include the following.

□ Matt Bishop, *Introduction to Computer Security*. Addison Wesley.
□ Dieter Gollmann, *Computer Security*, Wiley Publishers.
□ Jonathan Knudsen, *Java Cryptography*, O'Reilly Press.

Excellent books on computer security in general:

□ Bruce Schneier, Applied Cryptography, Wiley Publishers.
□ Ross Anderson, Security Engineering, `http://www.cl.cam.ac.uk/ rja14/book.html`

Also checkout: `http://security.stackexchange.com`,

# Logistics I

Two lectures each week, for Semester 1. These are currently scheduled as: Monday 9h00-10h00, WGB G02, and Tuesday 13h00-14h00, WGB G15. You are required to attend all lectures.

Some tutorials will be scheduled, during which I'm happy further clarify class material, discuss exam strategy, work on problem sheets, past exam questions, and so forth. You are expected to attend all tutorials.

Total marks for this course is 100, including 10 marks for continuous assessment (which will be in the form of one laboratory assignment and one in-class exercises (TBA). You are expected to complete all assessments.

Module Website hosted at `http://cs4.ucc.ie/moodle/`

If you decide to register for this module then you **must** sign up on the module website *before* the end of September 2014.

# Logistics II

Programming exercises give students the opportunity to use the Java cryptographic APIs to better understand the cryptographic protocols considered in lectures. The exercises require writing code to interact with a special grading server; assessment is straightforward: full marks for a correct interaction and repeated attempts are allowed.

An in-lab exercise will have maximum duration of 40 mins. These exercises will give students the opportunity to answer final-exam 'style' questions. Grades and feedback on answers will be given.

If you have a question regarding material covered in class then I prefer that you ask the question during lectures or tutorials so that everyone can benefit from the discussion.

# Logistics III (rough outline/subject to change)

Weeks and Lectures:

| | |
|---|---|
| **W1–W3** | Introduction to cryptography, attacks and applications |
| **W4,5** | Java crypto APIs, message digests |
| **W6–W8** | Authentication/Security protocols |
| **W9–W12** | Public key protocols |

Weeks and Assignments (exact deadlines announced in lectures):

| | |
|---|---|
| **W5** | Java Lab (5 marks) |
| **W7** | Problem Lab 2 (5 marks) |

The university will contact you about examination schedules.

# Final Examination

This module will be examined at the end of Semester I. This module is 5 ECTS credits. The exam paper is graded out of 90 marks with 10 marks for Continuous Assessment.

Past papers available on library website (also look for CS4253). Exam paper will be discussed at end of semester.

Exam questions cover: straightforward regurgitation of material; a reasonably familiar problem that requires application of knowledge, or intended to stretch the student with more challenging/unfamiliar problems.

The intention is that a student who can regurgitate material can pass; a student who not only ‘knows’ the material but can apply it in straightforward ways can achieve a second class honours student. A first class honours fits the two previous categories and can apply the knowledge in more challenging ways to trickier and unfamiliar problems.

# Semesterization

Schedule:
`http://www.ucc.ie/en/media/support/semesterisationproject/Key_dat`
This module will be examined at the end of Semester I (December 2014).

Semester I is organized as 12 weeks teaching, 1 week study plus 2 weeks examinations; everything related to CS4614 *must* be done during these 15 weeks, as scheduled.

According to National Framework of Qualifications guidelines and European Credit Transfer and Accumulation System (ECTS) Users Guide 2009 a 5-credit module can correspond to between 100 and 150 hours of student effort. This includes lectures, labs, tutorials and independent study. Therefore, you should typically spend at least 6.6 hours of your time per week on CS4614.

Don't get caught out by the change to Semesterization!

*"By failing to prepare, you are preparing to fail"* [Benjamin Franklin]

# Attendance

"Every student registered for a diploma or degree is expected to attend all lectures, tutorials, laboratory classes etc. In the case of absence through illness, a student must, if possible, give notice of each absence in writing to the Lecturer concerned and/or Head of Department responsible. In the case of such absence for more than four lecture days the student must, on resuming attendance, notify the Lecturer and/or Head of Department to do so, lodge a medical certificate with the Student Records and Examinations Office which in turn will be circulated to the Head of Department. A student will not be permitted to enter for an examination at the conclusion of a module if attendance at that module is not considered satisfatory by the Registrar and Vice-President for Academic Affairs following a report by the Lecturer concerned and/or Head of Department responsible for the module. The decision of the Registrar and Vice-President for Academic Affairs is subject to the appeal of the Academic Council of the University." In the event of illness or bereavement, students should contact the module co-ordinator in the first instance and submit relevant documentation to the Departmental Office.

# Informalities
# (an analogy of what we worry about)

# Pin Tumbler Locks

Formalities

Informalities

▷ Pin Tumbler Locks

Correct Key Inserted

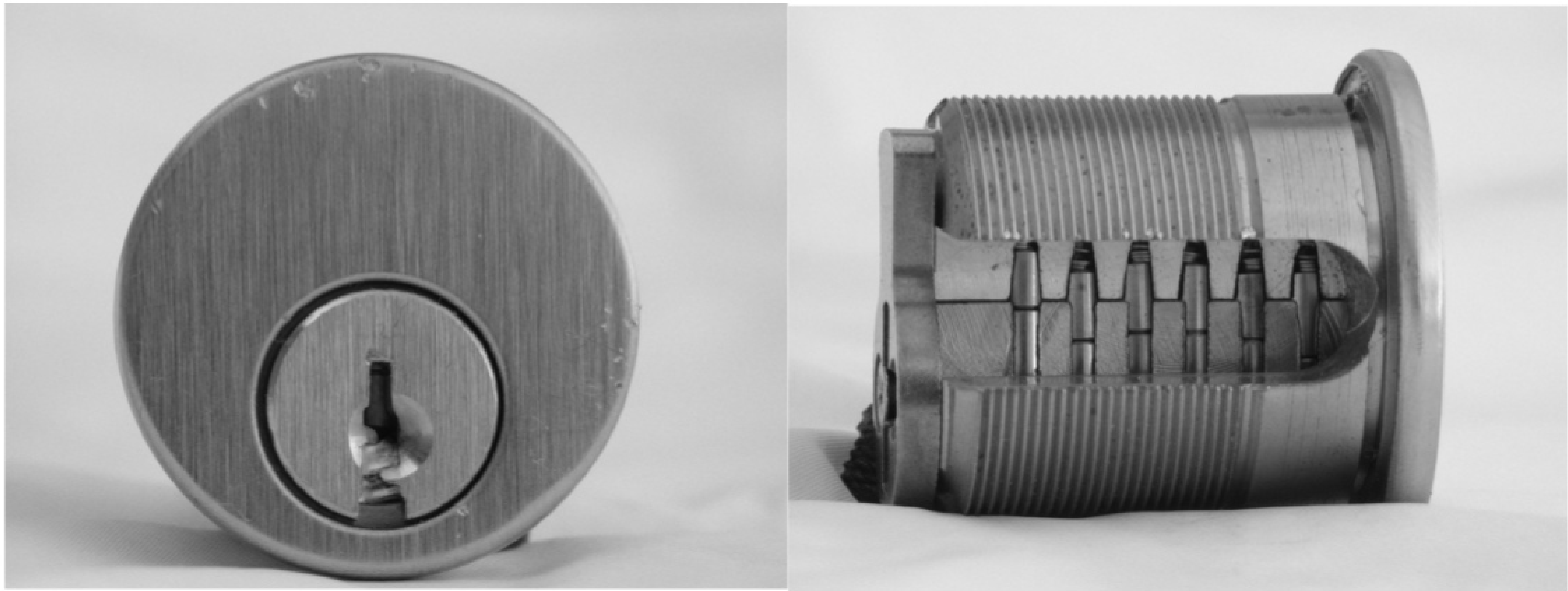
Incorrect Key Inserted

Guessing A Key for a Given Lock

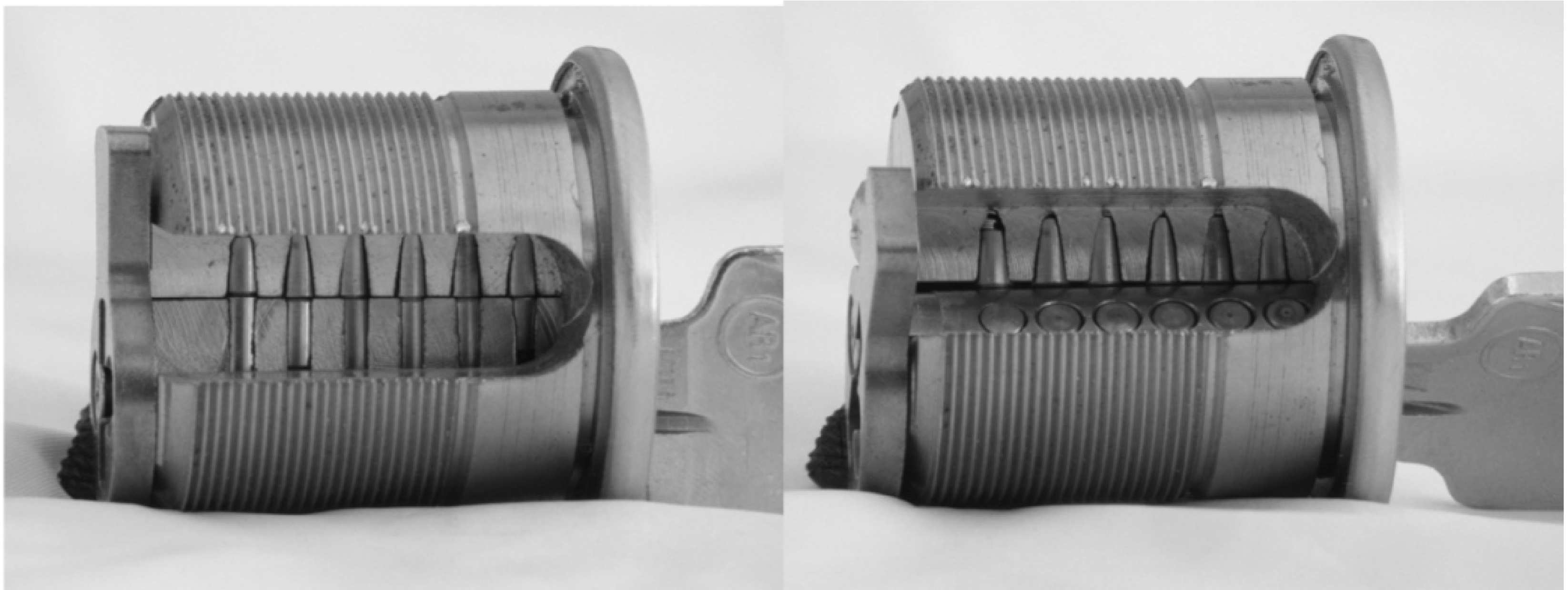
Lock Bumping

Master Keyed Pin Tumbler Lock

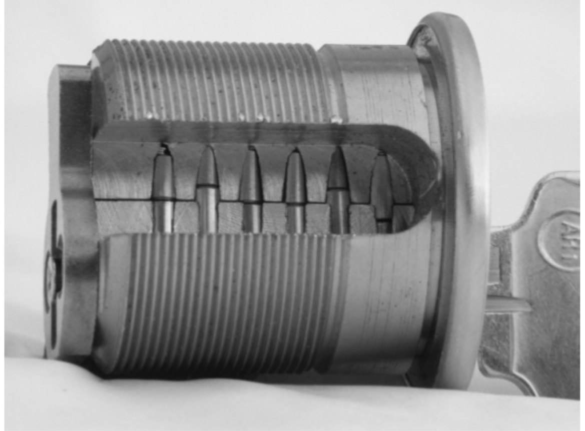
Master Key Attack



# Correct Key Inserted



# Incorrect Key Inserted



# Guessing A Key for a Given Lock

Formalities

Informalities

Pin Tumbler Locks

Correct Key Inserted

Incorrect Key Inserted

▷ Guessing A Key for a Given Lock

Lock Bumping

Master Keyed Pin Tumbler Lock

Master Key Attack

Difficulty depends on number of key-combinations, which is $D^P$, where

- $P$ number of pins (typically 4 to 7),
- $D$ number of possible pin depths (‘bitting depth’, typically between 4 and 10)

Goal is to make it impractical to test all possible key combinations (the key-space). Commercial locks have a key space between thousands and millions of keys.

For example, if it takes 1 min to cut one key for 5 pins (bitting depths of 10), then it will take $10^5$ mins to cut all keys, which is roughly 69 days.

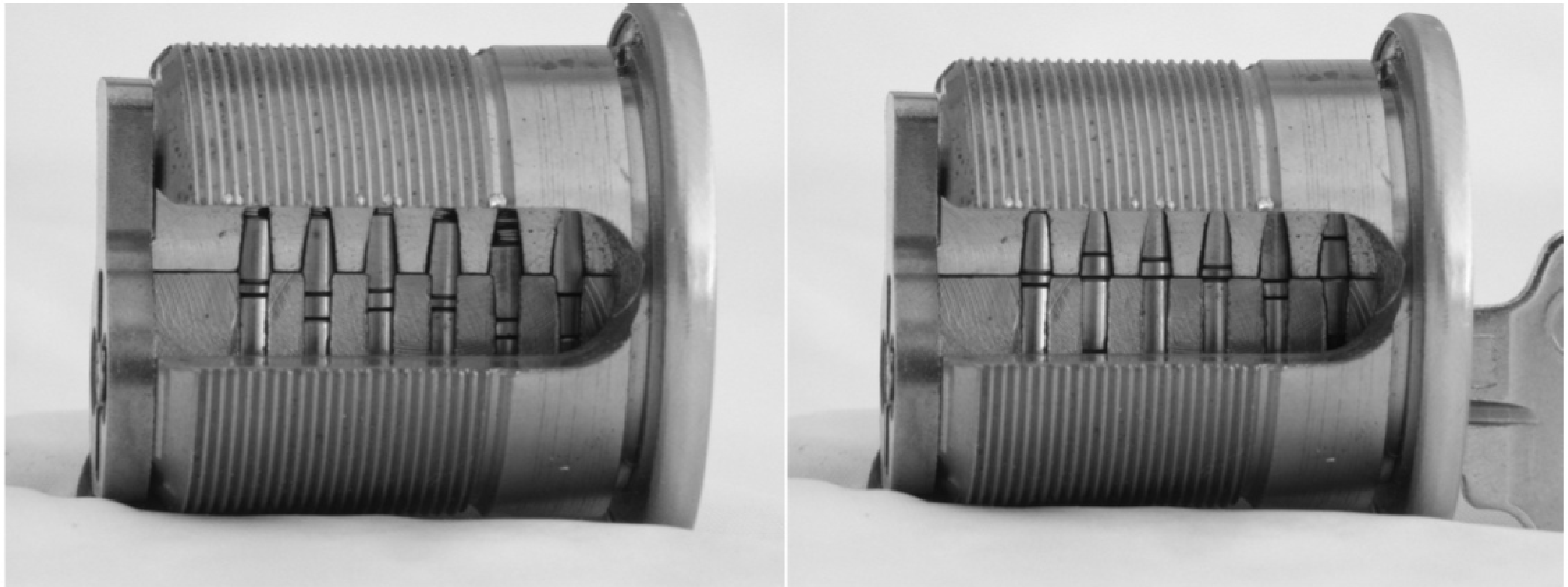
# Lock Bumping

(works with Acrobat Reader with Javascript enabled)

(click here)

[http://www.youtube.com/watch?v=XQDR-DBQRfl]

# Master Keyed Pin Tumbler Lock



# Master Key Attack

Formalities
Informalities
Pin Tumbler Locks
Correct Key Inserted
Incorrect Key Inserted
Guessing A Key for a Given Lock
Lock Bumping
Master Keyed Pin Tumbler Lock
▷ Master Key Attack

I have my own key and I'd like to know the master key for the WGB.

Strategy. For each pin position $p$ from 1 to $P$:

- □ cut $D-1$ copies of my own key, with a different bitting depth for the given pin $p$: all other pin bitting depths should be same as the original.
- □ test these keys. Two should open the lock.
  - my original
  - a copy with pin $p$'s bitting depth corresponding to the other split in the pin.

I know now the position of the other splits, with effort $P \times (D-1)$ key cuts.

This kind of attack is called an *Adaptive Oracle Attack*; for the full details see `http://www.crypto.com/masterkey.html`