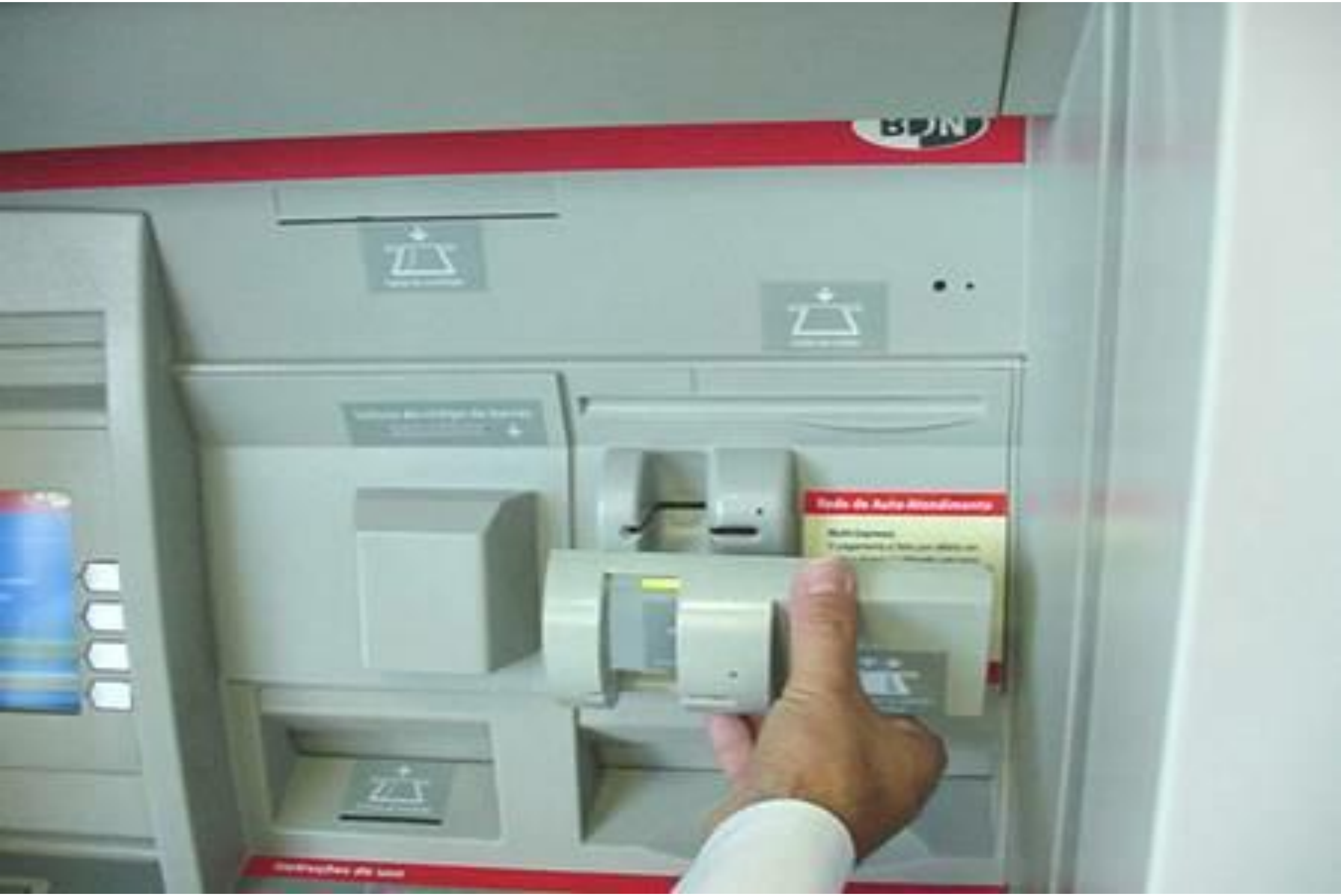
Software Security: Principles (Part Trois)

CS 161: Computer Security

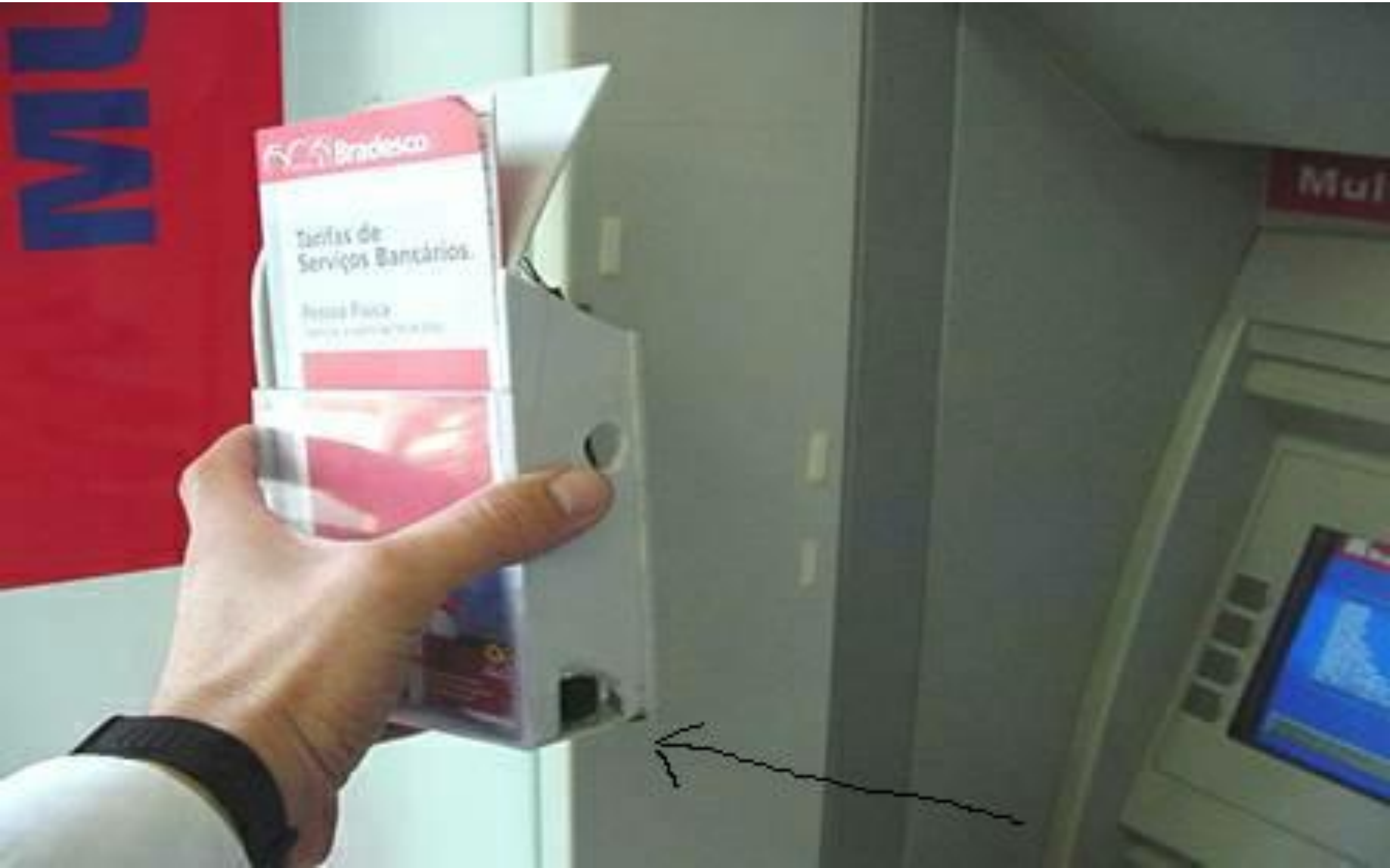
Prof. David Wagner

February 7, 2014

Leitura de código de barras
Bradesco
Instruções de uso

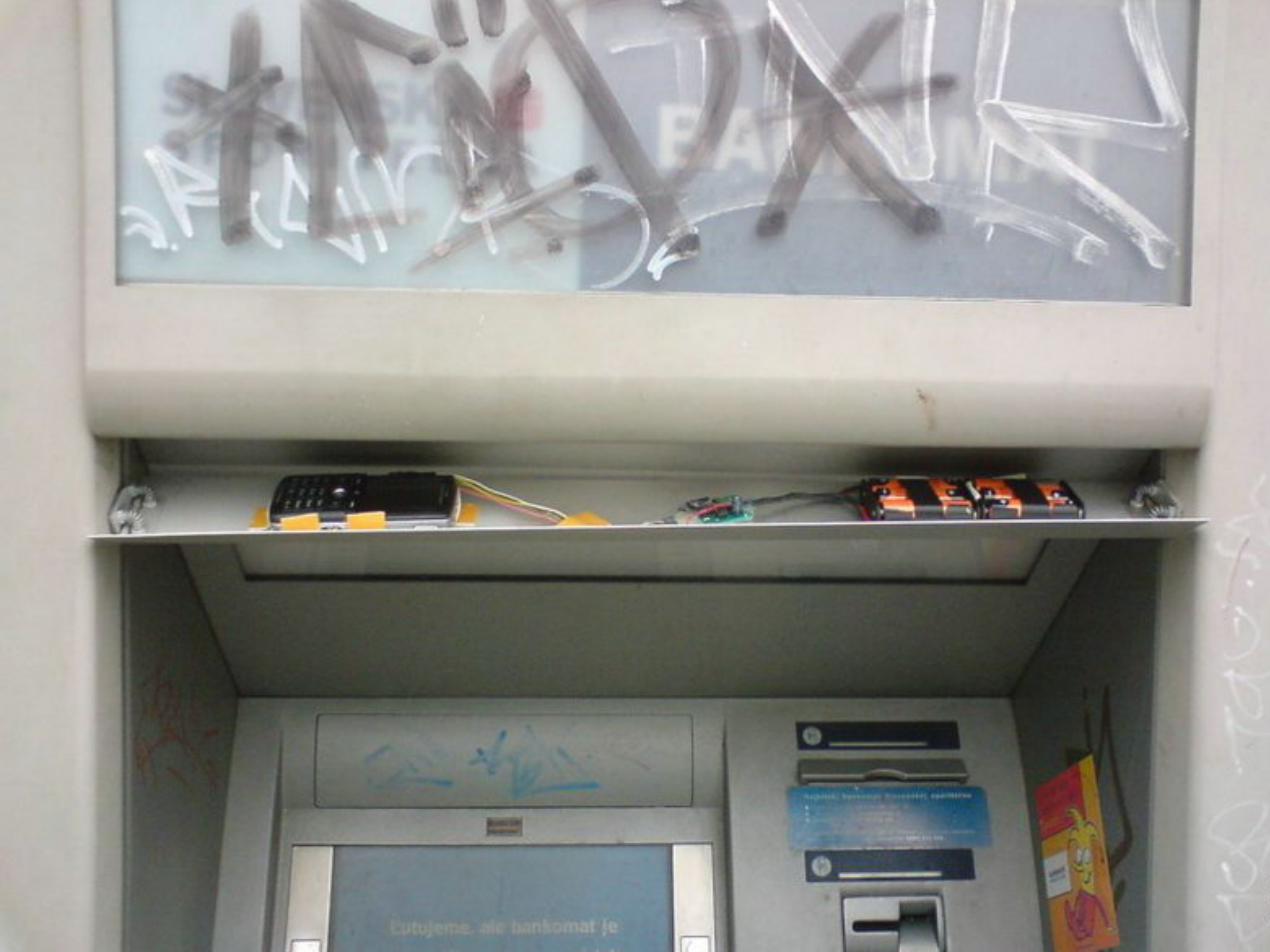

Sala de Auto-Atendimento

Bradesco
Tarifas de Serviços Bancários
Pessoa Física
Multi Expresso
Bradesco



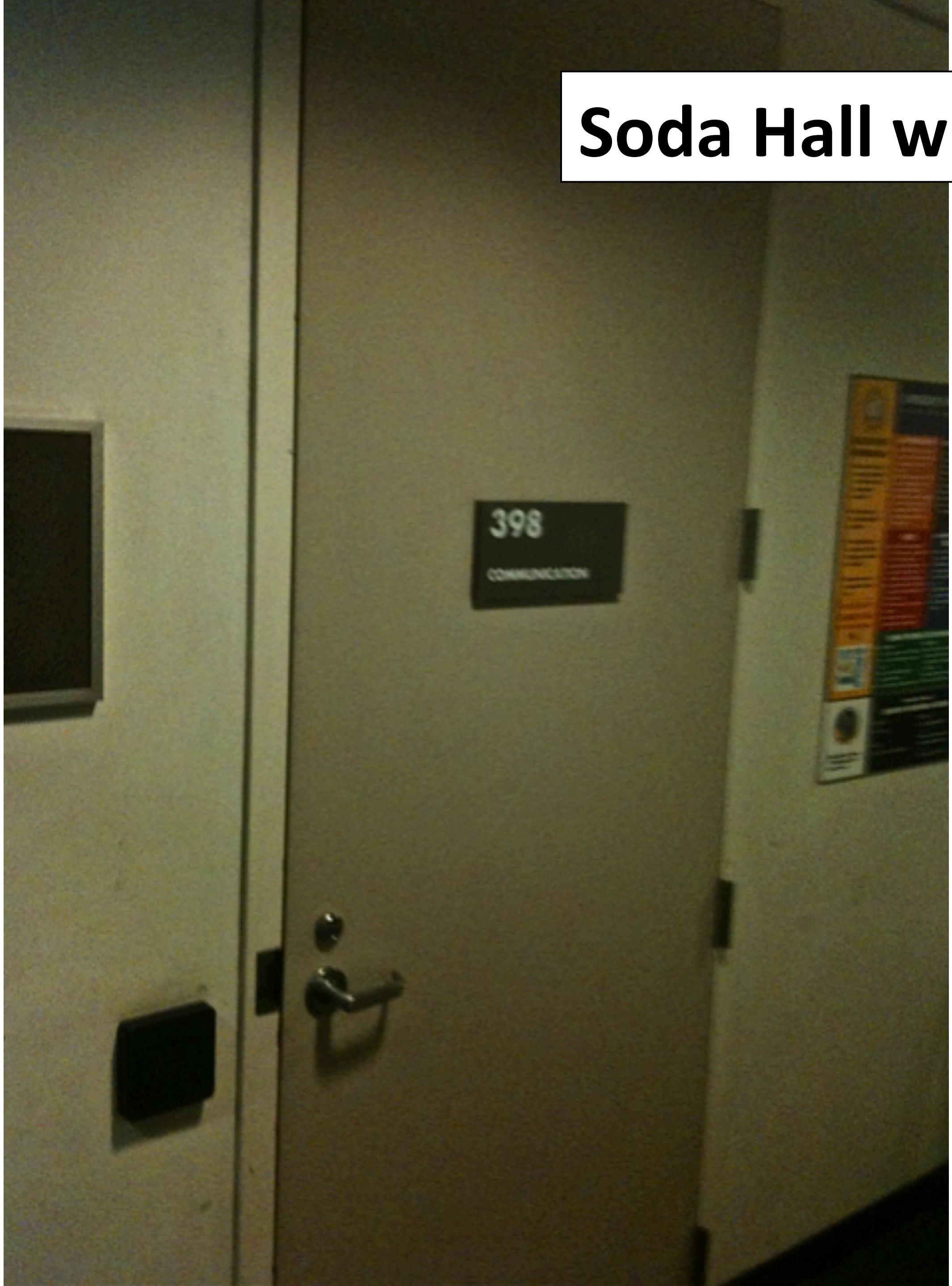
MU
Bradesco
Tarifas de Serviços Bancários.
Pessoa Física
Mul

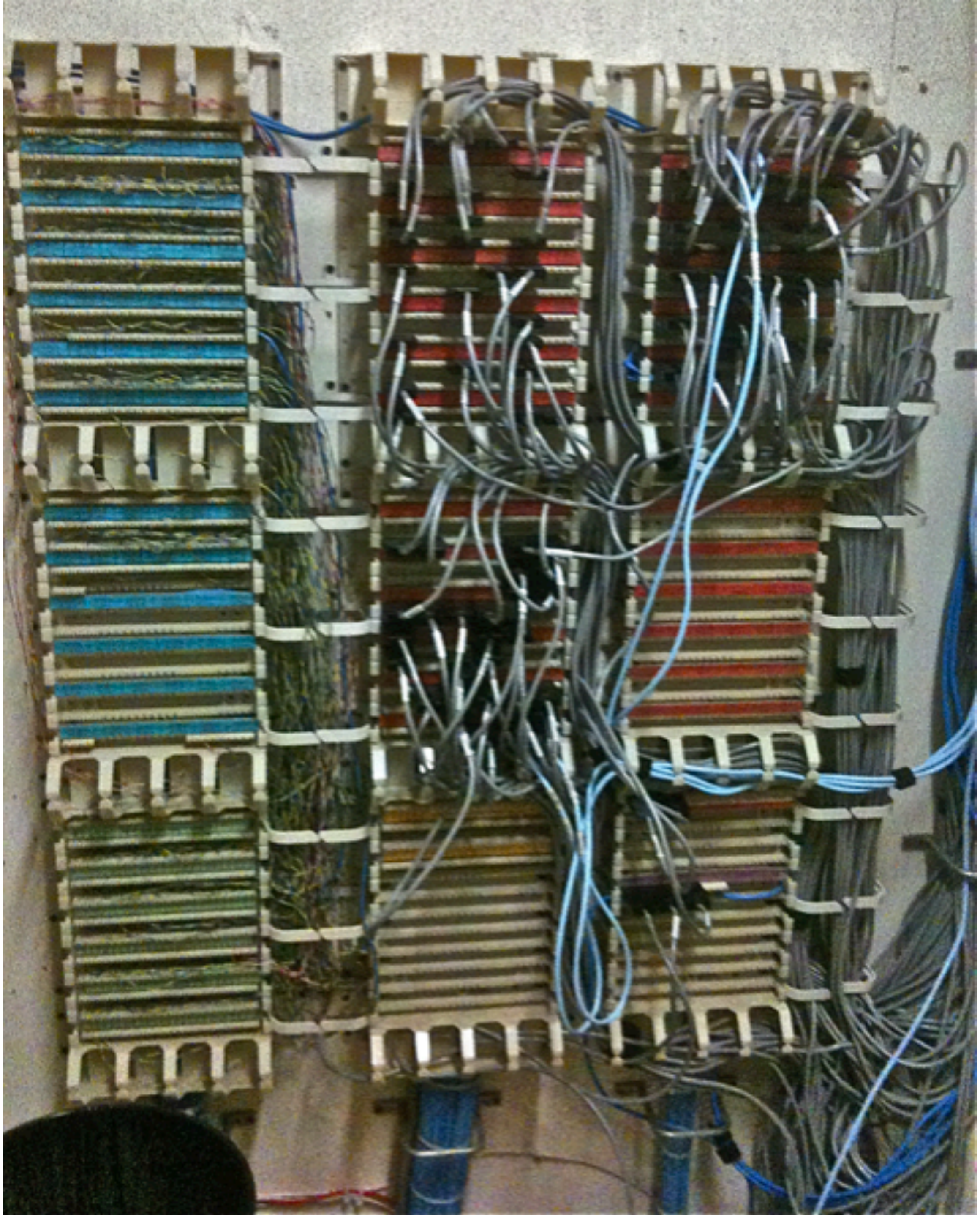
Ľutujeme, ale bankomat je
momentálne mimo prevádzky
We regret this ATM
is temporarily out of service

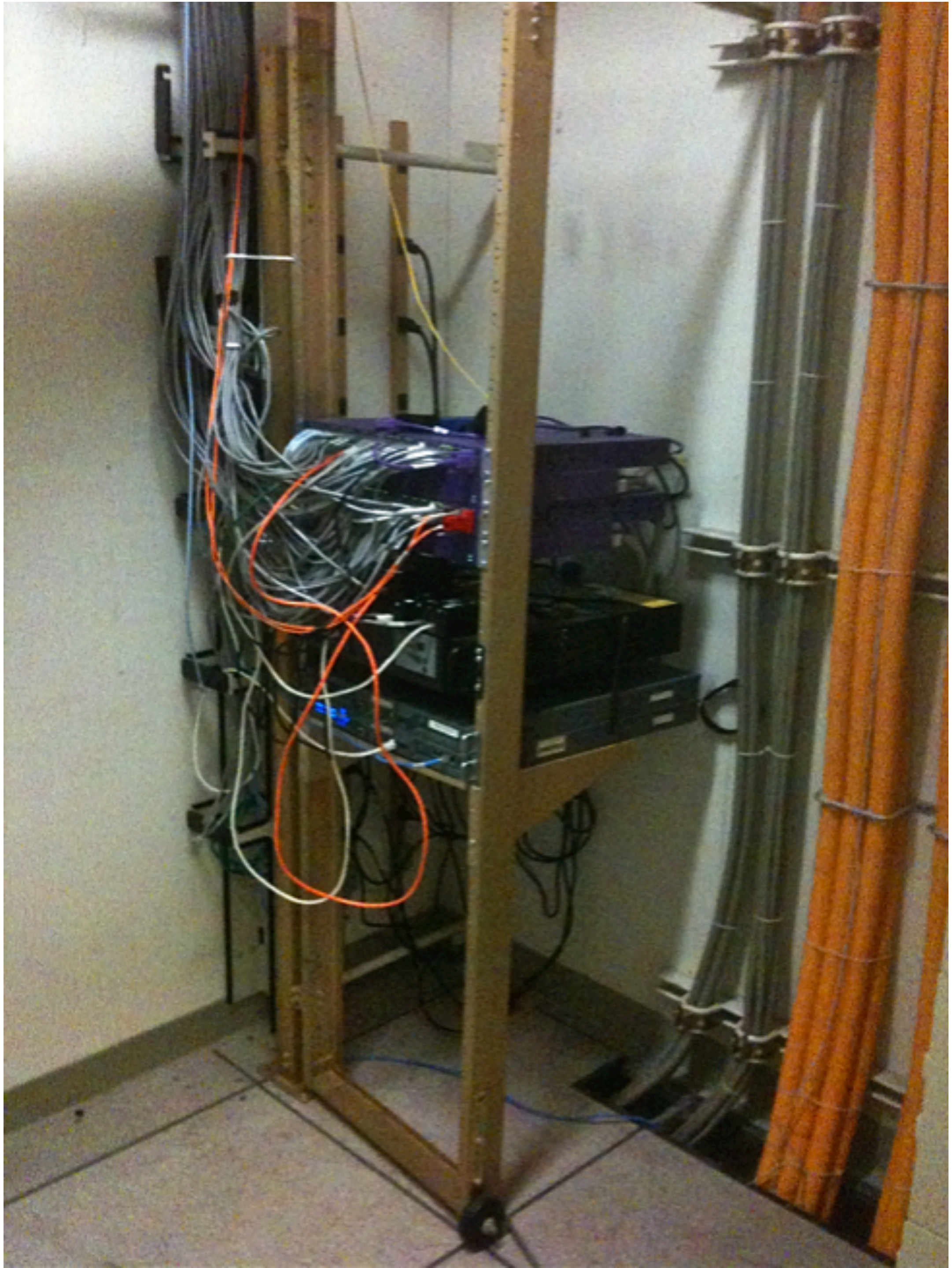

Ľutujeme, ale bankomat je

“Trusted path.”

Soda Hall wiring closet







Protection?

398
COMMUNICATION

“Use fail-safe defaults.”

GSA Container Classes Defined:

GSA: General Services Administration (US Government)

GSA Class 1:
a GSA approved container meeting Federal Specification AA-F-357(canceled) with entry protection consisting of 10 Man-Minutes forced entry, 30 Man-Minutes surreptitious entry and 1 hour fire rating

GSA Class 2:
a GSA approved container meeting Federal Specification AA-F-357(canceled) with entry protection consisting of 5 Man-Minutes forced entry, 20 Man-Minutes surreptitious entry and 1 hour fire rating

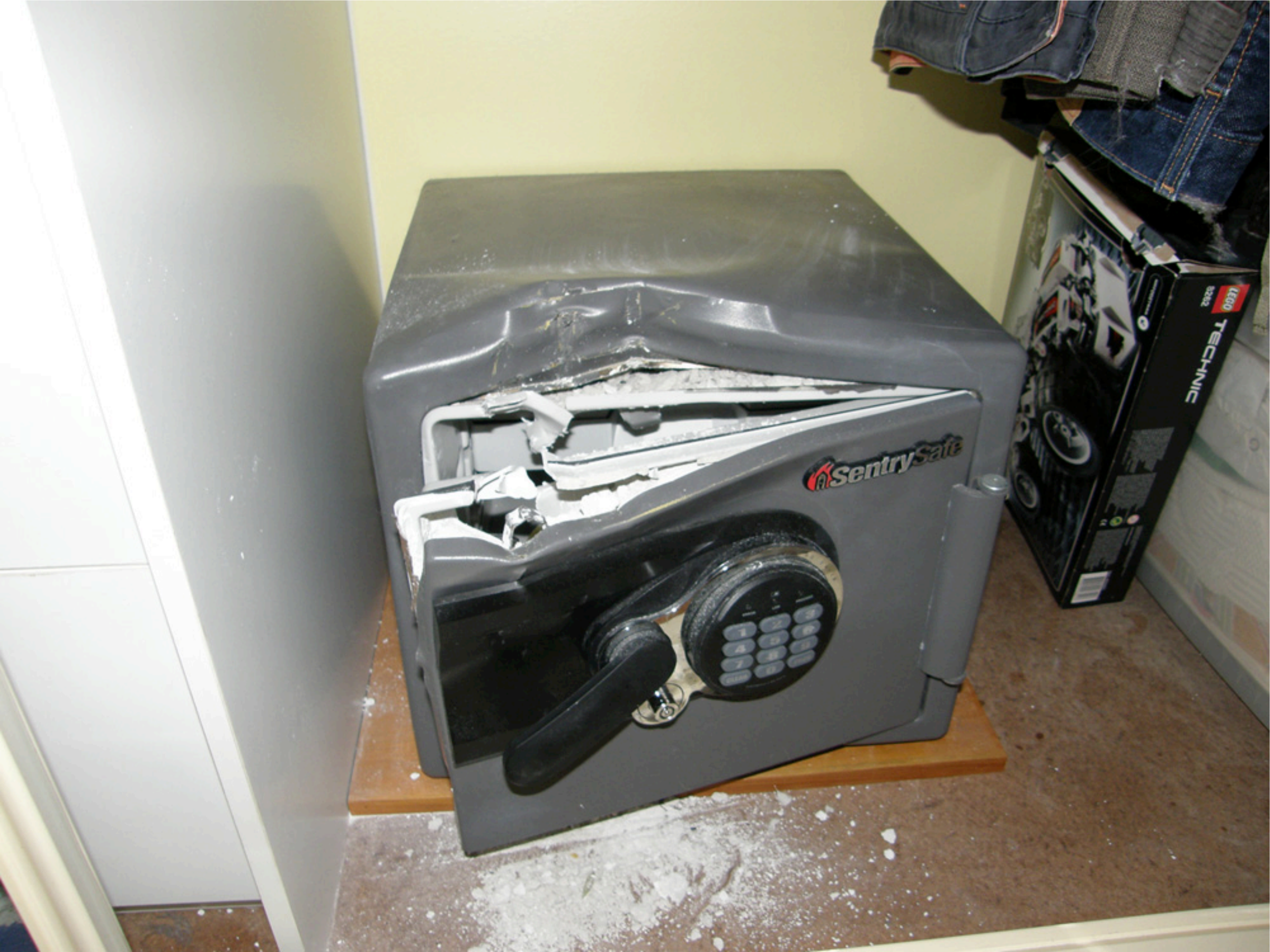
GSA Class 3:
a GSA approved uninsulated container meeting Federal Specification AA-F-358 with entry protection consisting of 20 Man-Minutes surreptitious entry

GSA Class 4:
a GSA approved uninsulated container meeting Federal Specification AA-F-358 with entry protection consisting of 5 Man-Minutes forced entry, 20 Man-Minutes surreptitious entry

Class 5 Four Drawer

GSA Class 5:
a GSA approved uninsulated container meeting Federal Specification AA-F-358 with entry protection consisting of 10 Man-Minutes forced entry, 20 Man-Hours surreptitious entry and 30 Man-Minutes Covert entry

GSA Class 6:
a GSA approved uninsulated container meeting Federal Specification AA-F-358 with entry protection consisting of 20 Man-Hours surreptitious entry and 30 Man-Minutes covert entry


SentrySafe
LEGO
TECHNIC

“Detect if you can’t prevent.”

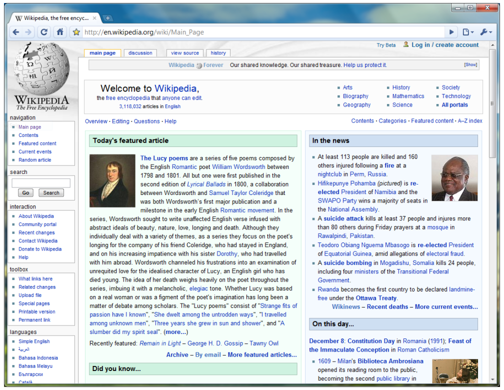
Summary

- Use *security thinking* – think like an attacker, identify architectural defenses
- You can practice this in everyday life!

Web Security

What is the Web?

- A platform for deploying applications, *portably* and *securely*



Wikipedia Forever Our shared knowledge. Our shared treasure. Help us protect it.

Welcome to Wikipedia,
the free encyclopedia that anyone can edit.
3,118,032 articles in English

Overview · Editing · Questions · Help

Contents · Categories · Featured content · A–Z index

Today's featured article

The Lucy poems are a series of five poems composed by the English Romantic poet William Wordsworth between 1798 and 1801. All but one were first published in the second edition of *Lyrical Ballads* in 1800, a collaboration between Wordsworth and Samuel Taylor Coleridge that was both Wordsworth's first major publication and a milestone in the early English Romantic movement. In the series, Wordsworth sought to write unaffected English verse infused with abstract ideals of beauty, nature, love, longing and death. Although they individually deal with a variety of themes, as a series they focus on the poet's longing for the company of his friend Coleridge, who had stayed in England, and on his increasing impatience with his sister Dorothy, who had travelled with him abroad. Wordsworth channeled his frustrations into an examination of unrequited love for the idealised character of Lucy, an English girl who has died young. The idea of her death weighs heavily on the poet throughout the series, imbuing it with a melancholic, elegiac tone. Whether Lucy was based on a real woman or was a figment of the poet's imagination has long been a matter of debate among scholars. The "Lucy poems" consist of "Strange fits of passion have I known", "She dwelt among the untrodden ways", "I travelled among unknown men", "Three years she grew in sun and shower", and "A slumber did my spirit seal". (**more...**)

Recently featured: *Remain in Light* – George H. D. Gossip – Tawny Owl

Archive – By email – **More featured articles...**

Did you know...

In the news

- At least 113 people are killed and 160 others injured following a **fire** at a nightclub in Perm, Russia.
- Hifikepunye Pohamba *(pictured)* is **re-elected** President of Namibia and the SWAPO Party wins a majority of seats in the National Assembly.
- A **suicide attack** kills at least 37 people and injures more than 80 others during Friday prayers at a mosque in Rawalpindi, Pakistan.
- Teodoro Obiang Nguema Mbasogo is **re-elected** President of Equatorial Guinea, amid allegations of electoral fraud.
- A **suicide bombing** in Mogadishu, Somalia kills 24 people, including four ministers of the Transitional Federal Government.
- Rwanda becomes the first country to be declared landmine-free under the **Ottawa Treaty**.

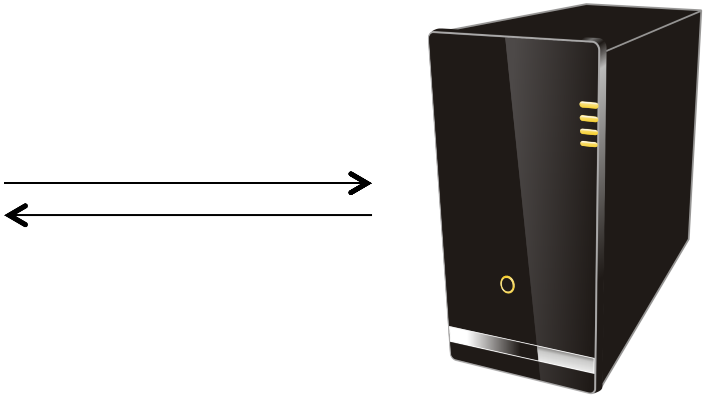
Wikinews – **Recent deaths** – **More current events...**

On this day...

December 8: **Constitution Day** in Romania (1991); **Feast of the Immaculate Conception** in Roman Catholicism

- 1609 – Milan's **Biblioteca Ambrosiana** opened its reading room to the public, becoming the second public library in

client



server

A historical perspective

- The web is an example of “bolt-on security”
- Originally, the web was invented to allow physicists to share their research papers
  - Only textual web pages + links to other pages; no security model to speak of
- Then we added embedded images
  - Crucial decision: a page can embed images loaded from another web server
- Then, Javascript, dynamic HTML, AJAX, CSS, frames, audio, video, …
- Today, a web site is a distributed application

Security on the web

- Integrity: malicious web sites should not be able to tamper with integrity of my computer or my information on other web sites
- Confidentiality: malicious web sites should not be able to learn confidential information from my computer or other web sites
- Privacy: malicious web sites should not be able to spy on me or my activities online

Security on the web

- Risk #1: we don't want a malicious site to be able to trash my files/programs on my computer
  - Browsing to `awesomevids.com` (or `evil.com`) should not infect my computer with malware, read or write files on my computer, etc.

Security on the web

- Risk #1: we don’t want a malicious site to be able to trash my files/programs on my computer
  - Browsing to `awesomevids.com` (or `evil.com`) should not infect my computer with malware, read or write files on my computer, etc.
- Defense: Javascript is sandboxed;
  try to avoid security bugs in browser code;
  privilege separation; automatic updates; etc.

Security on the web

- Risk #2: we don’t want a malicious site to be able to spy on or tamper with my information or interactions with other websites
  - Browsing to `evil.com` should not let `evil.com` spy on my emails in Gmail or buy stuff with my Amazon account

Security on the web

- Risk #2: we don’t want a malicious site to be able to spy on or tamper with my information or interactions with other websites
  - Browsing to `evil.com` should not let `evil.com` spy on my emails in Gmail or buy stuff with my Amazon account
- Defense: the same-origin policy
  - A security policy grafted on after-the-fact, and enforced by web browsers
  - Intuition: each web site is isolated from all others

Security on the web

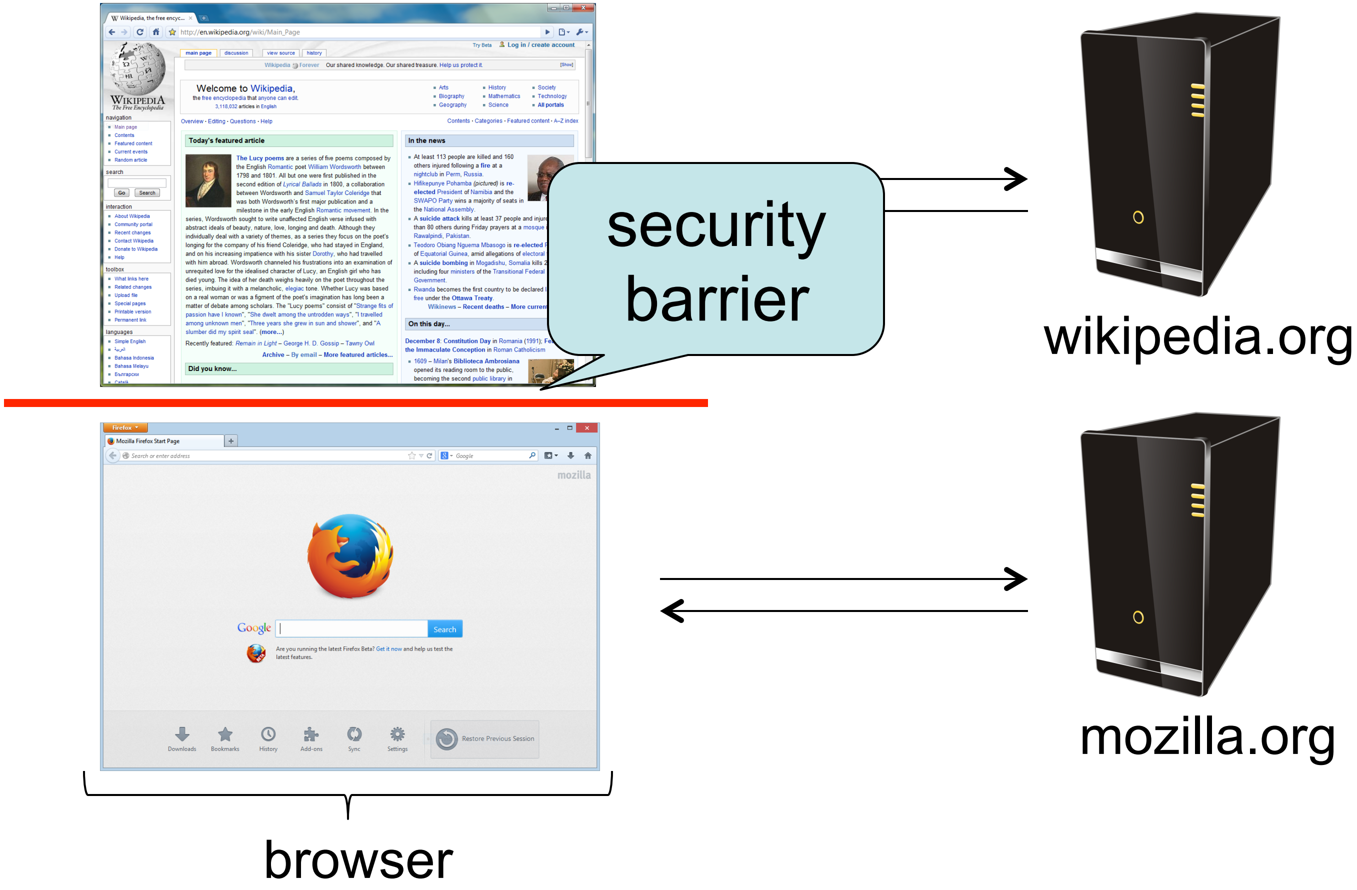
- Risk #3: we want data stored on a web server to be protected from unauthorized access

Security on the web

- Risk #3: we want data stored on a web server to be protected from unauthorized access
- Defense: server-side security

Same-origin policy

- Each site is isolated from all others



security barrier

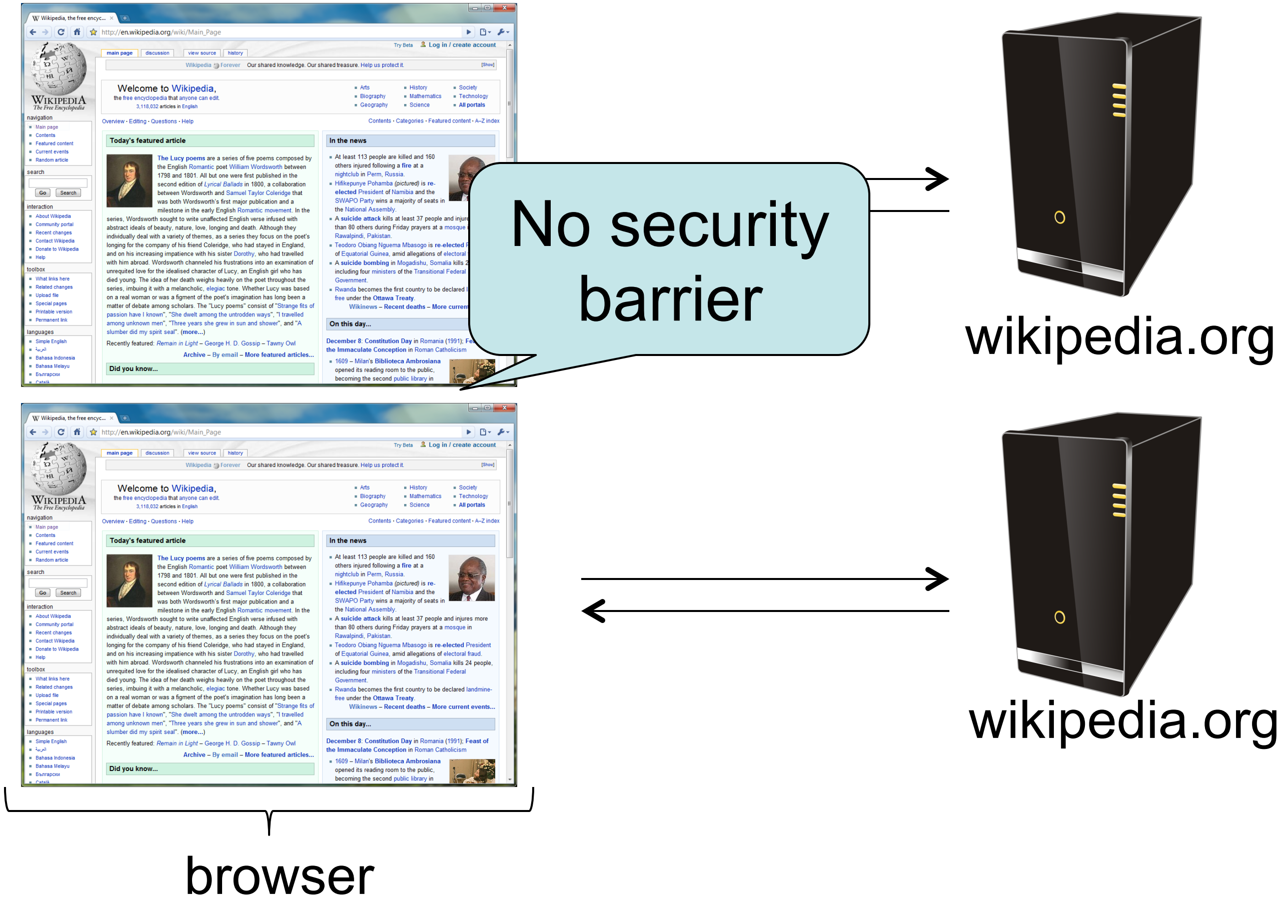
wikipedia.org

mozilla.org

browser

Same-origin policy

- Multiple pages from same site aren't isolated



No security barrier

wikipedia.org

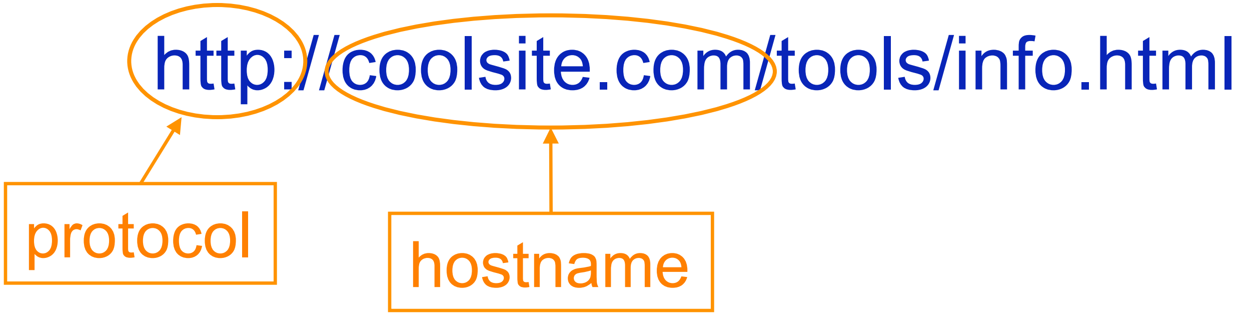
wikipedia.org

browser

http://en.wikipedia.org/wiki/Main_Page
http://en.wikipedia.org/wiki/Main_Page

Same-origin policy

- Granularity of protection: the *origin*
- Origin = protocol + hostname (+ port)



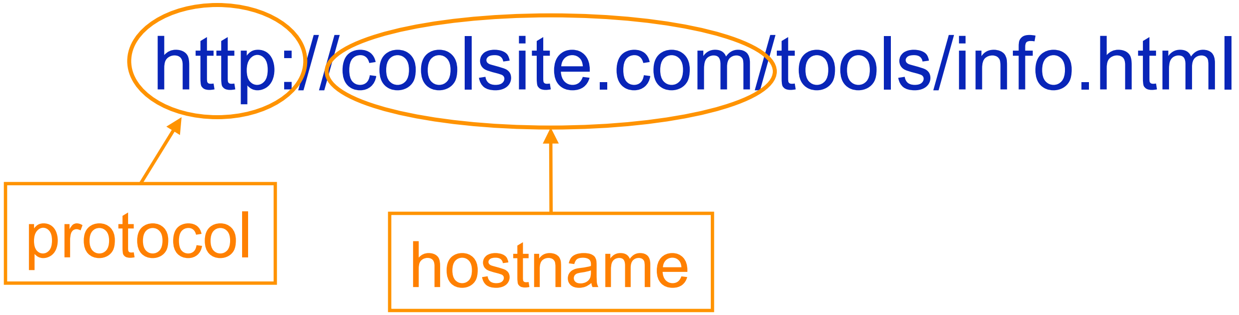
http://coolsite.com/tools/info.html

protocol

hostname

Same-origin policy

- Granularity of protection: the *origin*
- Origin = protocol + hostname (+ port)


http://coolsite.com/tools/info.html

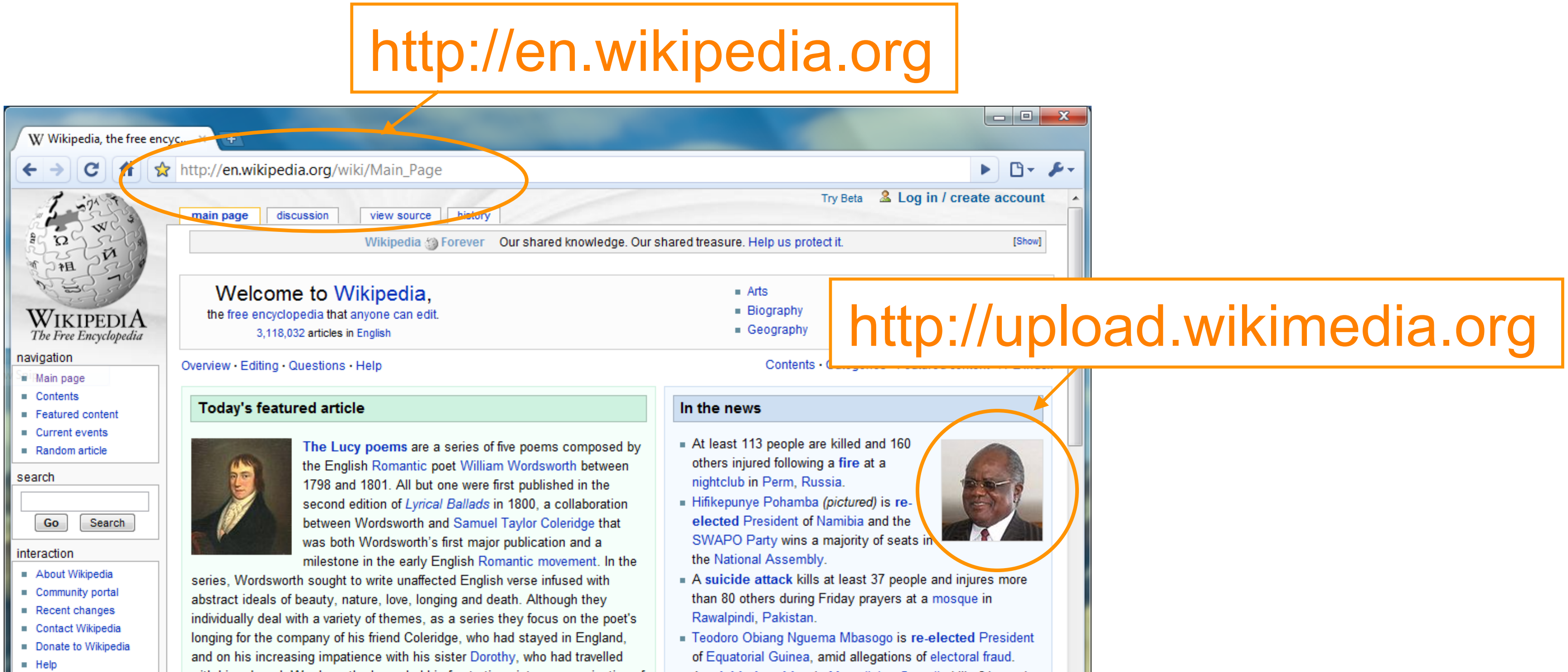
protocol

hostname

- Javascript on one page can read, change, and interact freely with all other pages from the same origin

Same-origin policy

- The origin of a page (frame, image, …) is derived from the URL it was loaded from



http://en.wikipedia.org

http://upload.wikimedia.org

Wikipedia Forever Our shared knowledge. Our shared treasure. Help us protect it.

Welcome to Wikipedia,

the free encyclopedia that anyone can edit.

3,118,032 articles in English

- Arts
- Biography
- Geography

Overview · Editing · Questions · Help

Contents ·

Today's featured article

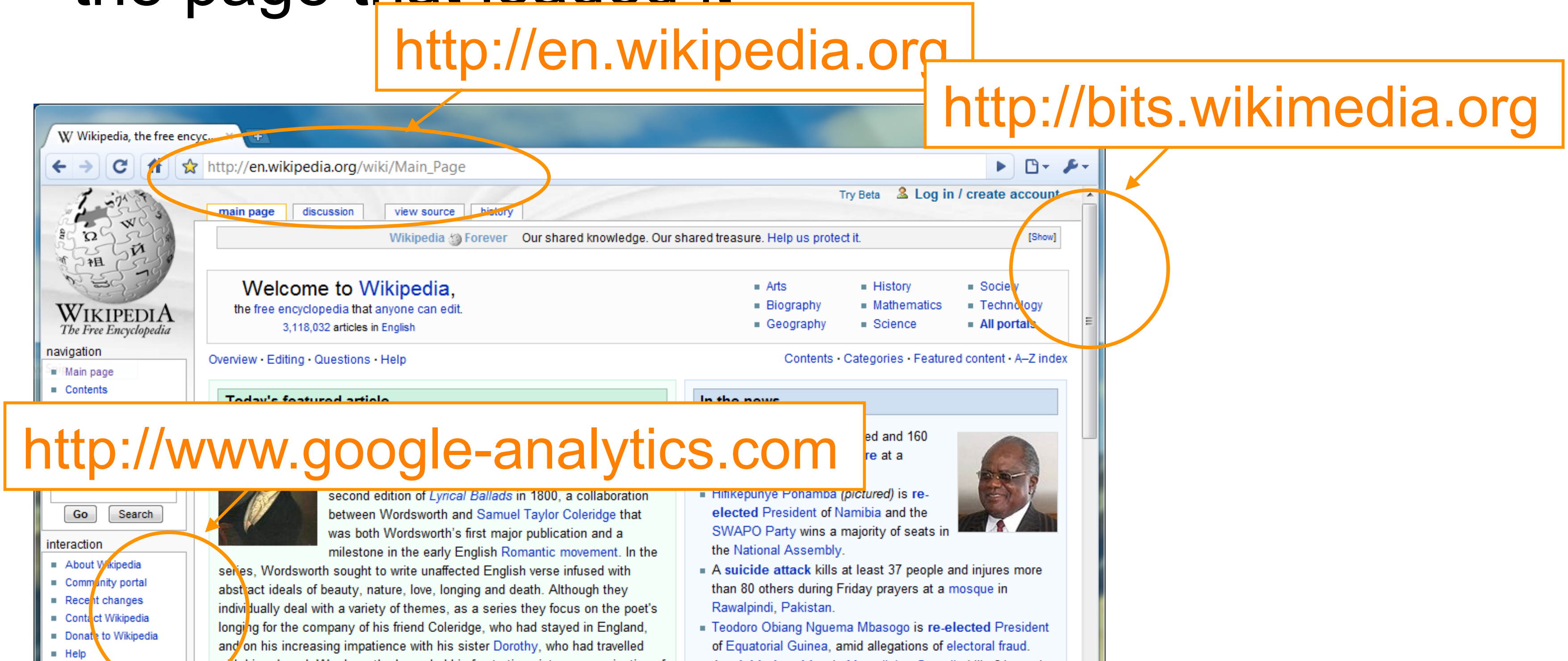
The Lucy poems are a series of five poems composed by the English Romantic poet William Wordsworth between 1798 and 1801. All but one were first published in the second edition of *Lyrical Ballads* in 1800, a collaboration between Wordsworth and Samuel Taylor Coleridge that was both Wordsworth's first major publication and a milestone in the early English Romantic movement. In the series, Wordsworth sought to write unaffected English verse infused with abstract ideals of beauty, nature, love, longing and death. Although they individually deal with a variety of themes, as a series they focus on the poet's longing for the company of his friend Coleridge, who had stayed in England, and on his increasing impatience with his sister Dorothy, who had travelled

In the news

- At least 113 people are killed and 160 others injured following a **fire** at a nightclub in Perm, Russia.
- Hifikepunye Pohamba *(pictured)* is **re-elected** President of Namibia and the SWAPO Party wins a majority of seats in the National Assembly.
- A **suicide attack** kills at least 37 people and injures more than 80 others during Friday prayers at a mosque in Rawalpindi, Pakistan.
- Teodoro Obiang Nguema Mbasogo is **re-elected** President of Equatorial Guinea, amid allegations of electoral fraud.

Same-origin policy

- The origin of a page (frame, image, …) is derived from the URL it was loaded from
- Special case: Javascript runs with the origin of the page that loaded it



http://en.wikipedia.org

http://bits.wikimedia.org

http://www.google-analytics.com

Wikipedia Forever Our shared knowledge. Our shared treasure. Help us protect it.

Welcome to Wikipedia,
the free encyclopedia that anyone can edit.
3,118,032 articles in English

- Arts
- Biography
- Geography
- History
- Mathematics
- Science
- Society
- Technology
- All portals

Overview · Editing · Questions · Help

Contents · Categories · Featured content · A–Z index

Today's featured article

second edition of Lyrical Ballads in 1800, a collaboration between Wordsworth and Samuel Taylor Coleridge that was both Wordsworth's first major publication and a milestone in the early English Romantic movement. In the series, Wordsworth sought to write unaffected English verse infused with abstract ideals of beauty, nature, love, longing and death. Although they individually deal with a variety of themes, as a series they focus on the poet's longing for the company of his friend Coleridge, who had stayed in England, and on his increasing impatience with his sister Dorothy, who had travelled

In the news

ed and 160 re at a

- Hifikepunye Pohamba (pictured) is re-elected President of Namibia and the SWAPO Party wins a majority of seats in the National Assembly.
- A suicide attack kills at least 37 people and injures more than 80 others during Friday prayers at a mosque in Rawalpindi, Pakistan.
- Teodoro Obiang Nguema Mbasogo is re-elected President of Equatorial Guinea, amid allegations of electoral fraud.

Coming up

- Attacks on web servers