Security & Privacy

… and why you should care.

Sarah Harvey
{CrySP, Information Retrieval} group
University of Waterloo
sharvey@cs.uwaterloo.ca

Why this talk?

Why this talk?

- Lots of media coverage on Snowden, NSA, and other government agencies
- Media coverage on sec/privacy policies companies
- Does the general public actually understand what all of this means?
- What are the implications of these findings?
  - Not just technological, but social context

Who am I?

- …mostly just some PhD student at UW
- Interested in Sec/Pri problems in IR systems
  - User profiling, user behavior
  - Privacy implications of profiling, linking
  - Improving privacy of large IR systems
- Interested promoting awareness of security, privacy systems

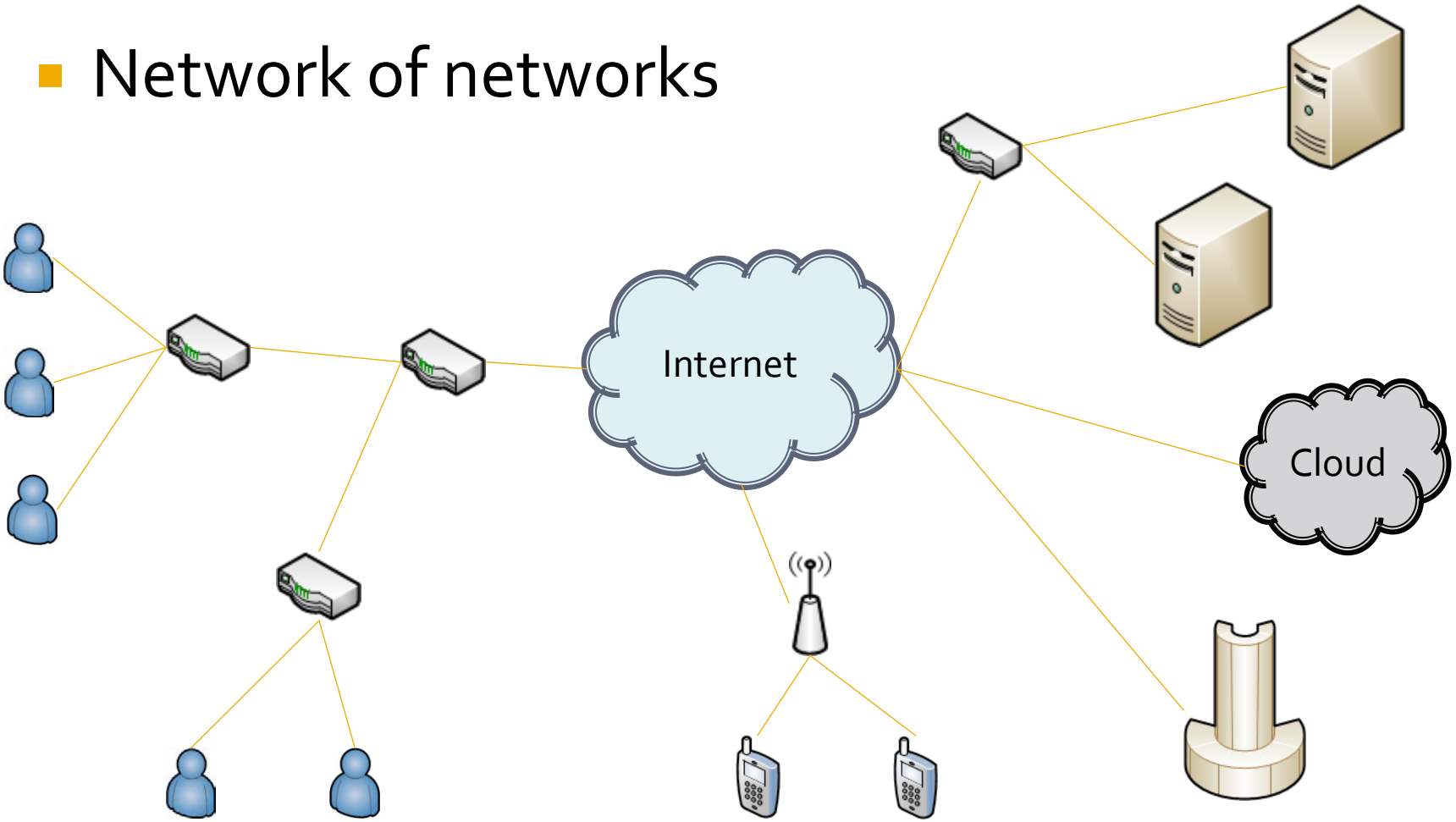
Outline

- Motivation
- What defines security? privacy?
- Who gets to see your stuff?
  - Who is the "bad guy"?
- Snowden and friends
- The issue of trust

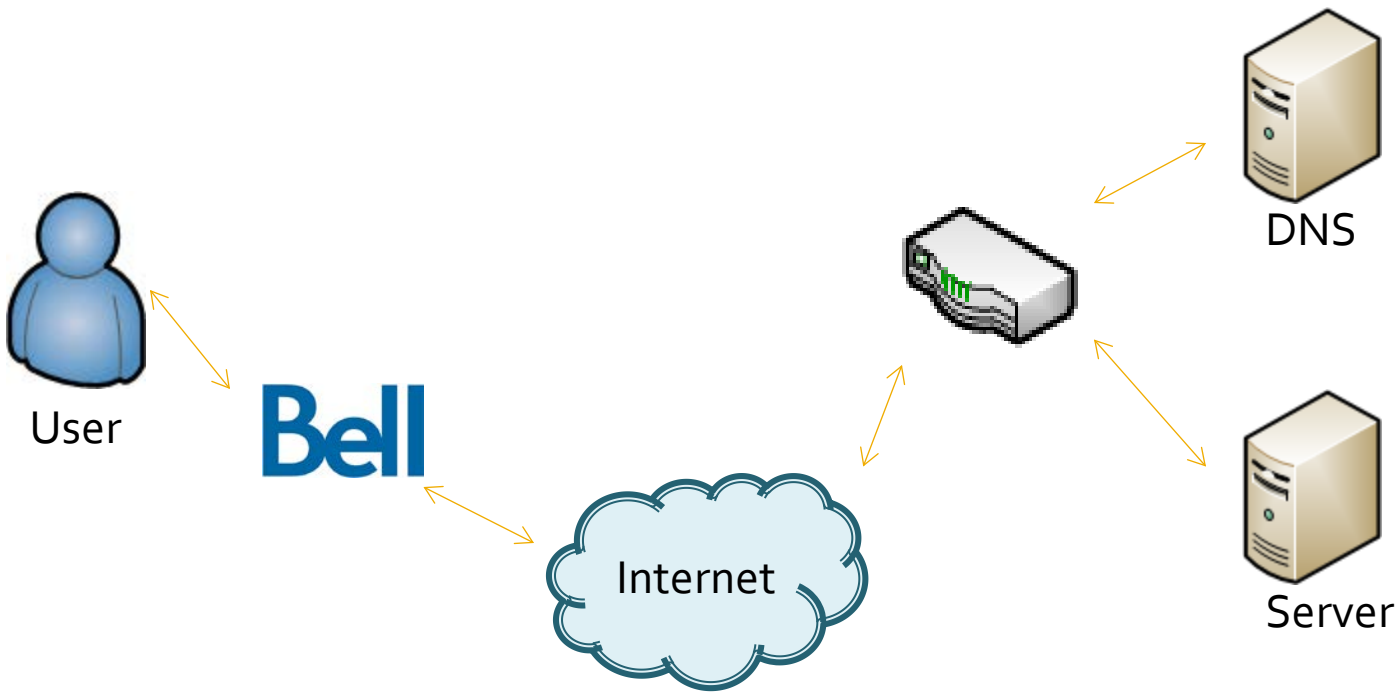
This, Jen... is the internet

What is the internet?

- Network of networks

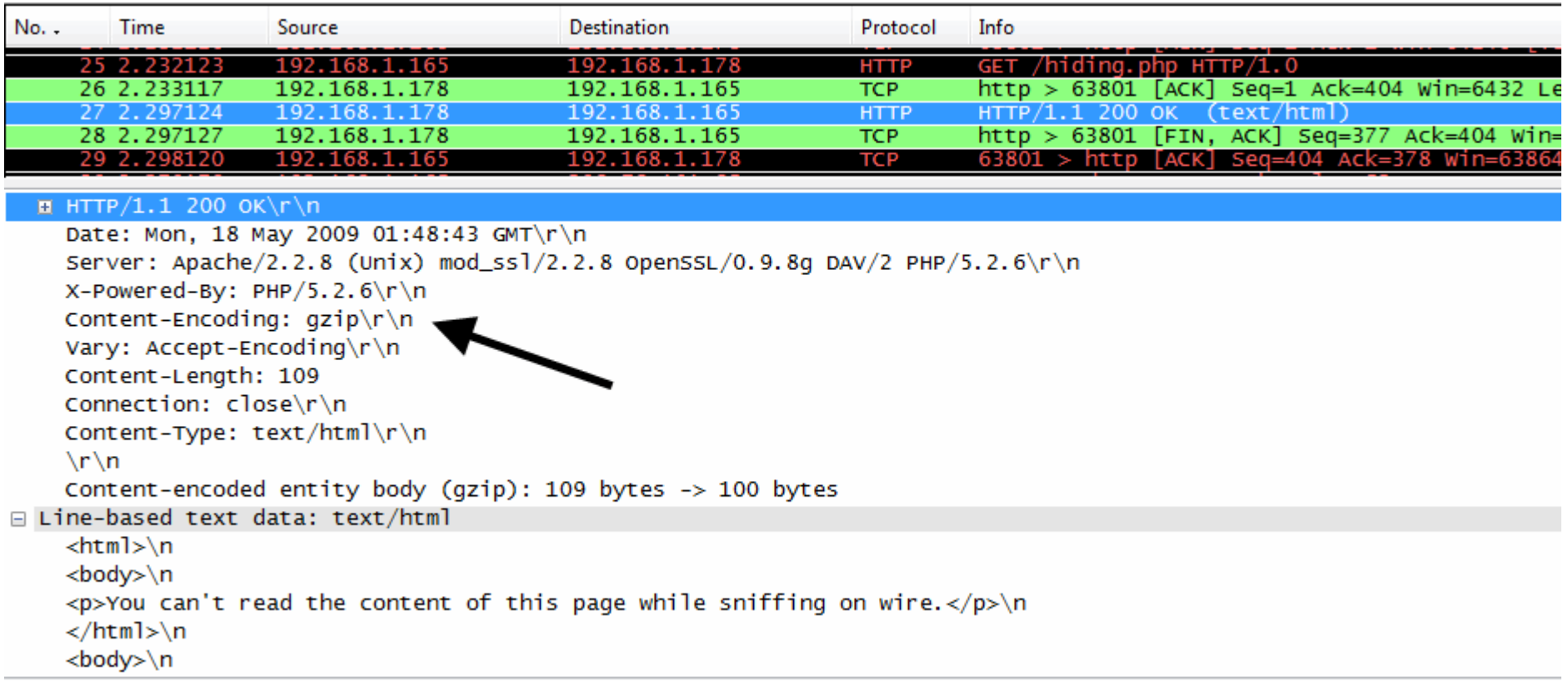


A typical internet pathway



What's on the wire?

- Any of those people can see my stuff

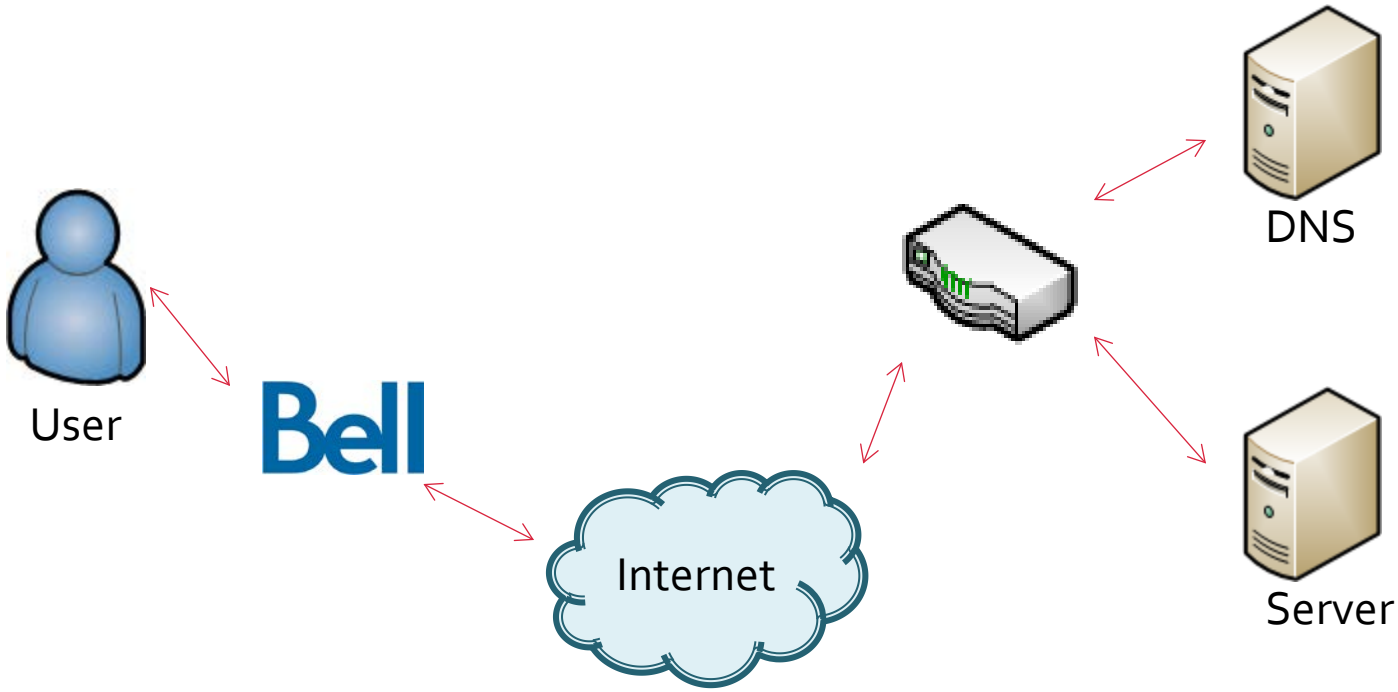


Cryptography in 30 seconds

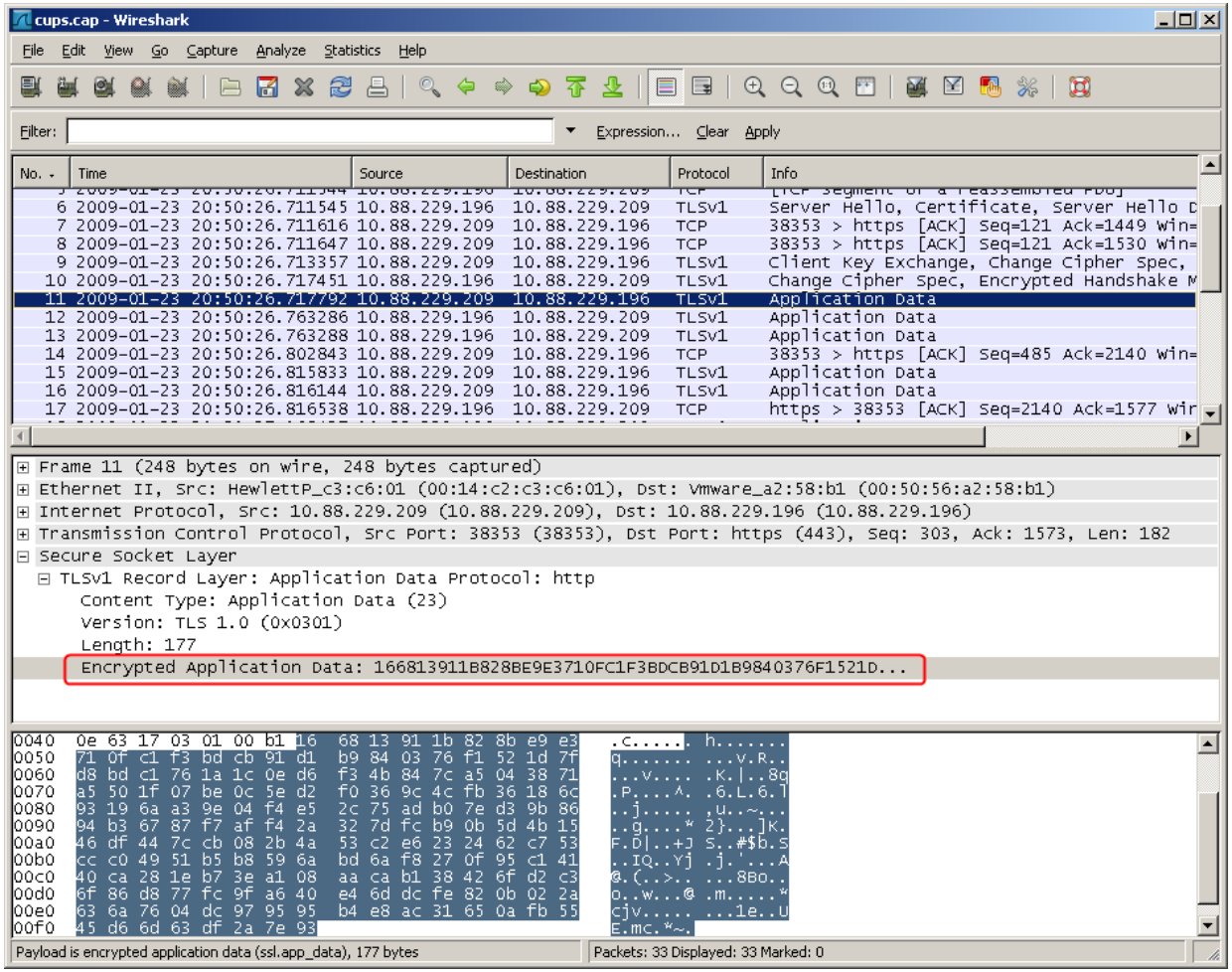
- So we have this wonderful technology called **cryptography**.
  - Encryption protects **confidentiality**.
  - MACs/digital signatures protect **integrity** and **authenticity**.
- Types of cryptographic systems:
  - Symmetric-key systems
  - Public-key systems

Applying crypto

- Revisiting communication securely



Revisiting the wire



Crypto in practice

- HTTPS (the green padlock in your browser)
  - HTTP with SSL
  - Doesn't hide endpoints
- SSH (host keys, transport, pub/pri keys)
  - Doesn't hide endpoints
- Mail (STARTTLS, PGP/GPG)
  - PGP/GPG doesn't protect mail headers

So…

- We're transmitting our data **securely**, but that doesn't mean our communication is necessarily **private**.

- Metadata is still being leaked:
  - Who we're talking to
  - When
  - What method (e.g. thing ports/protocol)

Definitions in 30 seconds

- Security is the **practice of** defending information from unauthorized parties
  - Prevent use, tampering, duplication, destruction
- Privacy is the **ability to** seclude one's information from unauthorized parties

Is this really of concern?

- The communication itself is protected.
- Is the metadata really that useful?
- Is it possible to record all that information?

A different view

- Let's take a look at what other things we may inadvertently reveal:
  - Search/click habits (tied to a Google/Bing account)
  - Purchase habits (tied to a credit card, account)
  - Location habits (GPS, PRESTO card, etc.)
  - Etc.
- We are living in an age where any and all information is collected about us.

Do we need to be concerned?

- It depends on who the bad guy is.
- In security/privacy circles, we have a notion of identifying **who/what is our adversary.**
- We then make certain security assurances about **what we can secure/hide against the defined adversary**.

Recall how we're usually told to secure our systems:

- Don't go to the super sketchy websites
- Use antivirus
- Use firewall
- Don't reuse passwords
- Never put out personal information about yourself

- We're totally cool here, right guys?

Consider who the adversary is

- Case 1: scriptkiddies and co.
  - Target: home machines/routers
  - Purpose: Pwn ur PC (for fun ~~and profit~~)
  - Purpose: create botnets, zombie PCs, etc.
  - Method: various scripts/packages readily available (e.g. Metasploit)

Consider who the adversary is

- Case 2: identity thieves
  - Target: accounts of specific users
  - Purpose: look for personal information for financial gain
  - Method: OSInt, specific backdoors, phishing

Consider who the adversary is

- Case 3: government agencies
  - Target: whistleblowers (the physical person)
  - Purpose: prevent highly classified/sensitive information from being revealed
  - Method: <CLASSIFIED>

Consider who the adversary is

- Case 4: corporations
  - Target: everyone
  - Purpose: improve services for all users; research
  - Method: marketing, lax policies, privacy guarantees
  - Method: scanning through consumed content

Why does this all matter?

- We knowingly or unknowingly end up **providing a large amount of information** about ourselves
- We now have systems that are capable of both **storing** and **analyzing** this data
  - (This is the focus of information retrieval systems)
- We often **trust** major third parties to **do the right thing** in order to provide us with **useful services**

Speaking of third parties…

Former NSA Honcho Calls Corporate IT Security "Appalling"

Posted by **samzenpus** on Thursday October 03, 2013 @12:35AM
from the is-that-better-than-terrible? dept.

Nerval's Lobster writes

> "Former NSA technology boss Prescott Winter has a word for the kind of security he sees

Snowden affair

Snowden affair

- Leaked a number of documents suggesting government surveillance programs in place:
  - PRISM
  - XKeyscore
  - Tempora
- Called the most significant leak in US history

Companies response:

- Nope.
- There is no way that **Microsoft, Google, Facebook, Apple, etc.** would willingly provide the NSA with information.
- Policies exist to protect the user, right?

Haha no.

BUSINESS INSIDER

BI INTELLIGENCE

Tech | Finance | Politics | Strategy | Life | Entertainment

TECH

More: Yahoo Marissa Mayer NSA PRISM

Marissa Mayer: 'It's Treason' For Yahoo To Disobey The NSA

JULIE BORT | SEP. 11, 2013, 6:06 PM | 32,764 | 105

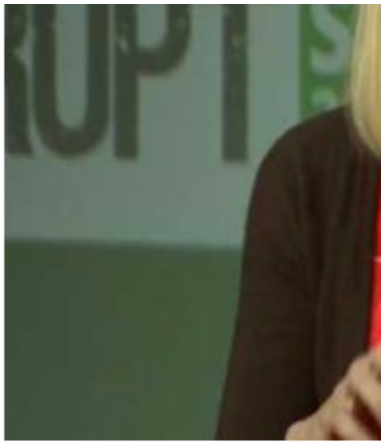
Recommend 1.7k | Share 27 | Tweet 646 | +1 79 | EMAIL | MORE

Marissa Mayer was on stage on Wednesday at the TechCrunch Disrupt conference when Michael Arrington asked her about NSA snooping.

Haha no.

He wanted to know what would happen if Yahoo just didn't cooperate. He wanted to know what would happen if she were to simply talk about what was happening, even though the government had forbidden it.

"Releasing classified information is treason. It generally lands you incarcerated," she said, clearly uncomfortable with the turn of the conversation.



Yahoo CEO Marissa Mayer

YHOO	Oct 08 04:39PM
32.93	

Clearly we can trust crypto

PCWorld Macworld TechHive

SECURITY security, privacy

Silent Circle ditches NIST cryptographic standards to thwart NSA spying

Lucian Constantin, IDG News Service

Oct 2, 2013 6:36 AM

The U.S. National Security Agency's reported efforts to weaken encryption standards have prompted an encrypted communications company to move away from cryptographic algorithms sanctioned by the U.S. National Institute of Standards and Technology (NIST).

Silent Circle, a provider of encrypted mobile Voice over Internet Protocol (VoIP) and text messaging apps and services, will stop using the Advanced Encryption Standard (AES) cipher and Secure Hash Algorithm 2 (SHA-2) hash functions as default cryptographic algorithms in its products.

...or trust Linux

(Mis)Uses of Technology

by Glyn Moody

Thu, Sep 19th 2013 1:44pm

Linus Torvalds Admits He Was Approached By US Government To Insert Backdoor Into Linux -- Or Does He?

from the *who-can-you-trust?* dept

At the LinuxCon meeting in New Orleans, Linus Torvalds was asked if he had ever been approached by the US government to insert a backdoor into the Linux kernel. Here's his characteristic answer:

> *Torvalds responded "no" while shaking his head "yes," as the audience broke into spontaneous laughter.*

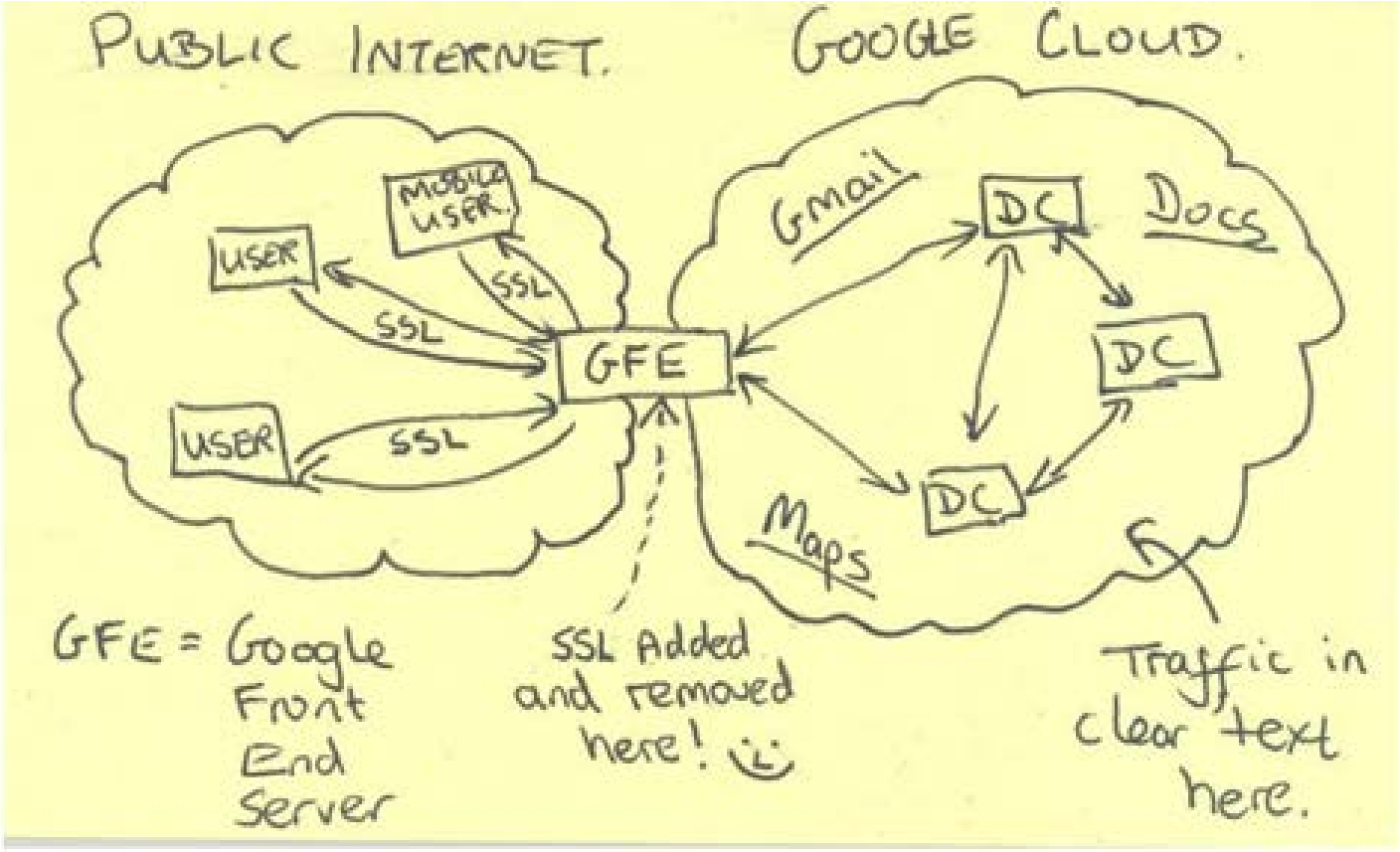
So why do we care?

- We can't just worry about protecting explicit information
  - Lots of implicit information being leaked
- Our data is subject to… who's whims?
  - Hackers?
  - Corporations?
  - Gov't Agencies?
- We may not be threats to national security, but we should be aware that this is happening, and be guaranteed some level of privacy

Two recent things to think about

- Adobe leak:
  - Big company = millions of users
  - Source code compromised
  - Passwords were encrypted, **not hashed**
- NSA v. The World:
  - German Chancellor Merkel's phone was **tapped**
  - NSA reveals to be monitoring the links between **users** and **corporate datacenters**

SSL Added and Removed here!



Questions? Open Discussion

http://teespring.com/nsassl