Week 4

CS 3923/CS 6813 Computer Security/Information Security & Privacy

Security Policies

[*] Slides based upon materials maintained by Justin Cappos at NYU

Week 4

Security Policy

- A security policy is a set of rules stating which actions are permitted and which are not.
- Can be informal or highly mathematical.
- If we consider a computer system to be a finite state automaton with state transitions, then
  - A *security policy* is a statement that partitions the states of a system into a set of authorized or secure states and a set of unauthorized or non-secure states.
  - A *secure system* is a system that starts in an authorized state and cannot enter an unauthorized state.
  - A *breach of security* occurs when a system enters an unauthorized state.
- We expect a trusted system to enforce the required security policies.

Week 4

Definitions

- There is no standard definition of security policy.
- Some define them as documents for humans to read:
  - The SANS Institute defines a security policy as "a document that outlines specific requirements or rules that must be met...usually point-specific, covering a single area.”
  - SearchSecurity.com: "In business, a security policy is a document that states in writing how a company plans to protect the company's physical and information technology (IT) assets.”
  - ISO17799: “To provide management direction and support for information security”

NYU

Week 4

Definitions (continued)

- But in other contexts, machine readable instructions are also called policy:
  - The term “firewall policy” is typically used for the firewall rule set
  - Crypto policy (acceptable algorithms, key lengths) are used in IPSec Security Association (SA) negotiations
  - Machine readable policies all derive from text-based policies, and should just be machine readable versions of human readable policies (possibly with detail added)
- Many documents about policy focus on policies for users and employees (e. g., acceptable use policies)
- We take a broad view of what a policy is, but focus on “human readable policies”

Week 4

Confidentiality, Integrity and Availability

- *Confidentiality:* Let *X* be a set of entities and *I* be some information. Then *I* has the property of confidentiality with respect to *X* if no member of *X* can obtain information about *I*.
- *Integrity:* Let *X* be a set of entities and *I* some information. Then *I* has the property of integrity with respect to *X* if *I* is unmodifiable by *X*.
- *Availability:* Let *X* be a set of entities and *I* a resource. Then *I* has the property of availability with respect to *X* if all members of *X* can access *I*.

Week 4

Elements of a Security Policy

- A security policy considers all relevant aspects of confidentiality, integrity and availability.
  - Confidentiality policy: Identifies information leakage and controls information flow.
  - Integrity Policy: Identifies authorized ways in which information may be altered. Enforces separation of duties.
  - Availability policy: Describes what services must be provided: example – a browser must be able to download pages but may optionally choose not to execute JavaScript.

Week 4

Mechanism and Policy

- Mechanism should not be confused with policy.
- A security mechanism is an entity or procedure that enforces some part of a security policy.

Week 4

Mechanism or Policy?

NYU

Week 4

Mechanism or Policy?

Another warning sign cautions against FOD (Foreign Object Debris) and points visitors to lockers to stow their cameras, sunglasses and other items prior to riding. Click to enlarge.

NYU

Week 4

Types of Security Policies

- Two types of security policies have been well studied in the literature:
  - A *military security policy* (also called government security policy) is a security policy developed primarily to provide confidentiality.
    - Not worrying about trusting the object as much as disclosing the object
  - A *commercial security policy* is a security policy developed primarily to provide integrity.
    - Focus on how much the object can be trusted.
- Also called confidentiality policy and integrity policy.

NYU

Week 4

Security Models

- To formulate a security policy you have to describe entities it governs and what rules constitute it – a *security model* does just that!
- A *security model* is a model that represents a particular policy or set of policies. They are used to:
  - Describe or document a policy
  - Test a policy for completeness and consistency
  - Help conceptualize and design an implementation
  - Check whether an implementation meets requirements.

Week 4

The Bell-La Padula (BLP) Model

- BLP model is a formal description of allowable paths of information flow in a secure system.
- Formalization of military security policy – confidentiality.
- Set of subjects S and objects O. Each subject s in S and o in O has a fixed security class L(s) (clearance) and L(o) (classification).
- Security classes are ordered by a relation
- Combines mandatory and discretionary access control.

Example

Top Secret (TS)	Dean Jelena	Strategic Files
Secret (S)	Prof. Gerig	Personnel Files
Confidential (C)	Susana	Student Files
Unclassified (UC)	Prof. Cappos	Class Files

A basic confidentiality classification system. The four levels are arranged on the list from most sensitive at top and least sensitive at bottom. In the middle are individuals grouped by their *security clearance* and at the right are documents grouped by their *security level*.

So Prof. Cappos can read class files and Dean Jelena can read any file. But what if Dean Jelena reads contents of personnel files and writes them onto the CS392 class file?

Week 4

BLP – Simple Version

- Two properties characterize the secure flow of information:
  - *Simple Security Property:* A subject s may have read access to an object o if and only if L(o) <= L(s) and s has discretionary read access to o.

    (Security clearance of subject has to be at least as high as that of the object).
  - *-Property: A subject s who has read access to an object o may have write access to an object p only if L(o) <= L(p) and s has discretionary write access to o.

    (Contents of a sensitive object can only be written to objects at least as high. That is, prevent write-down).

NYU

BLP – Simple Version (Contd.)

- Basic Security Theorem: Let there be a system with a secure initial state and let T be a set of transformations . If every element of T preserves the simple security property and *-property, then every state is secure.

Week 4

BLP - Communicating with Subjects at a Lower Level

- If Alice wants to talk to Bob who is at a lower level how does she write a message to him?
- BLP allows this by having notion of maximum-security level and current security level.
- Maximum security level must dominate current security level.
- A "trusted subject" may effectively decrease its security level
  - This effectively ignores the *-Property

Week 4

Tranquility Principle

- Recall: BLP assumed that security levels of objects are constant.
- Principle of tranquility states that subjects and objects may not change their security level once instantiated.
- Principle of strong tranquility states that security levels do not change during the lifetime of the system.
- Principle of weak tranquility states that security levels do not change in a way that violates the rules of a given security policy.

Week 4

What about other properties?

What property does BLP protect?

What other properties are desirable?

NYU

Week 4

Biba Integrity Model (intuition)

- Protect **integrity**, not confidentiality

Core concept: "no read down, no write up"

- One cannot read a lower level
- One cannot write a higher level

Week 4

Biba Integrity Model (intuition)

- A General may write orders to a Colonel, who can issue these orders to a Major. In this fashion, the General's original orders are kept intact, and the mission of the military is protected (thus, "no read down" integrity). Conversely, a Private can never issue orders to his Sergeant, who may never issue orders to a Lieutenant, also protecting the integrity of the mission ("no write up"). [Wikipedia]

Week 4

Biba Integrity Model

- Biba integrity model is counterpart (dual) of BLP model.
- It identifies paths that could lead to inappropriate modification of data as opposed to inappropriate disclosure in the BLP model.
- A system consists of a set *S* of subjects, a set *O* of objects, and a set *I* of integrity levels. The levels are ordered.
- Subjects and Objects are ordered by the integrity classification scheme; denoted by I(s) and I(o).

Week 4

What is wrong with Biba and BLP?

- Guarantees seem unrealistic
- Principles perform all operations
  - "Who" actually computes?
- Does this apply to the real world?

Week 4

Chinese Wall Model

- The Chinese Wall Model is a model of a security policy that speaks equally to confidentiality and integrity. It describes policies that involve a conflict of interest in business. For example:
  - In the environment of a stock exchange or investment house the goal of the model is to prevent a conflict of interest in which a trader represents two clients, and the best interests of the client's conflict, so the trader could help one gain at the expense of the other.

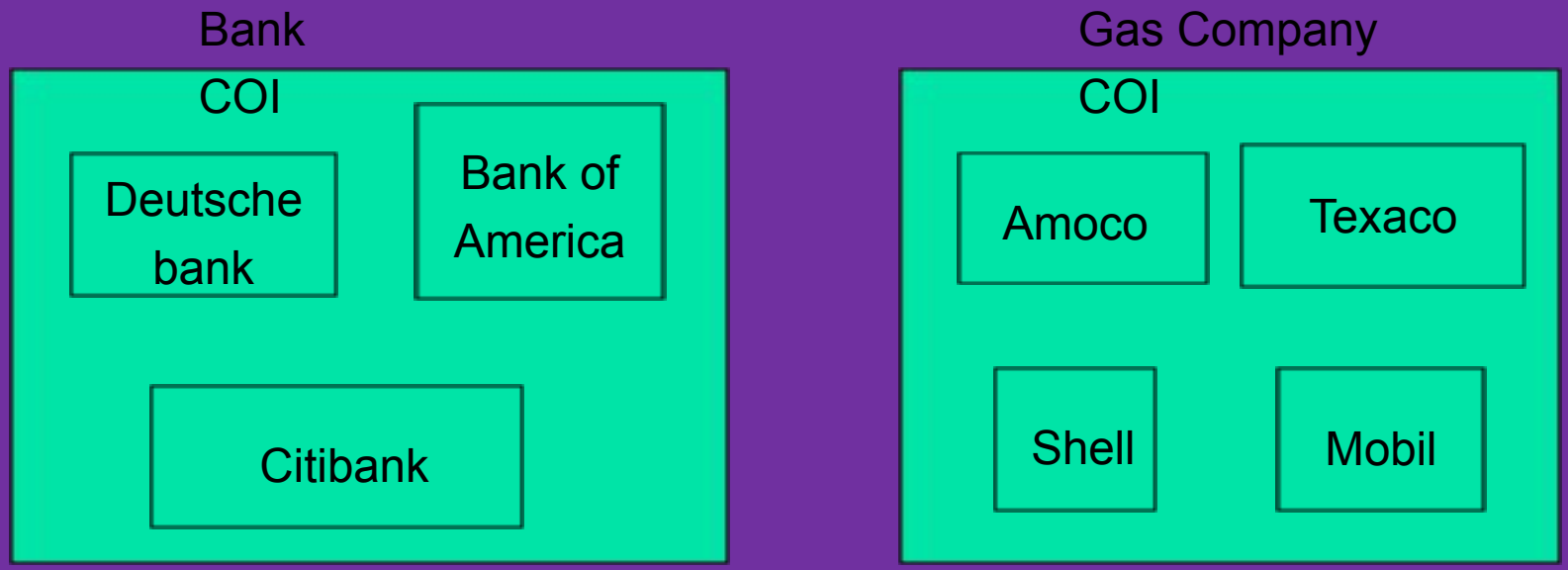
Week 4

Chinese Wall Model

- The *objects* of the database are items of information related to a company.
- A *company dataset* (CD) contains objects related to a single company.
- A *conflict of interest* class (COI) contains the datasets of companies in competition.
- *COI*(O) represents the conflict of interest class that contains object O.
- *CD*(O) represents the company dataset that contains object O. The model assumes that each object belongs to exactly one conflict of interest class.

Week 4

Chinese Wall Model



Anthony has access to the objects in the CD of Bank of America. Because the CD of Citibank is in the same COI as that of Bank of America, Anthony cannot gain access to the objects in Citibank's CD. Thus, this structure of the database provides the required ability.

NYU

Chinese Wall Model

- Suppose Anthony and Susan work in the same trading house. Anthony can read objects in Bank of America's CD, and Susan can read objects in Citibank's CD. Both can read objects in Amoco's CD. If Anthony can also write objects in Amoco's CD, then he can read information from objects in Bank of America's CD, write it to objects in Amoco's CD, and then Susan can read that information;
- ***CW-* Property Rul***e: A subject *S* may write to an object *O* if and only if all of the following conditions hold:
  - The CW-simple security rule permits *S* to read O; and
  - For all unsanitized objects O', *S* can read O' => *CD*(O') = *CD*(O).

Week 4

How does one limit access?

Many cases access is necessary

- But not necessarily full / permanent access

Examples:

- Doctor access to health records
- Government access to ISP / telephone records
- Police access to criminal record

NYU

Week 4

Critical Information Systems Security Policy

- Policy for health information systems (Anderson).
- A *patient* is the subject of medical records, or an agent for that person who can give consent for the person to be treated.
- *Protected Health Information* is information about a patient's health or treatment enabling that patient to be identified.
- A *clinician* is a healthcare professional who has access personal access to personal health information while performing their jobs.

NYU

Week 4

Access Principles

- Each medical record has an access control list naming the individuals or groups who may read and append information to the record. The system must restrict access to those identified in the list.
- One of the clinicians on the access control list (*responsible* clinician) must have the right to add other clinicians to the access control list.
- The responsible clinician must notify the patient of the names on the access control list whenever the patient's medical record is opened. Except for situations given in Statutes or in cases of emergency the responsible clinician must obtain the patient's consent.

NYU

Week 4

Security Policies in Practice

- A security policy is essentially a document stating security goals, and which actions are required, which are permitted, and which are allowed.
  - Policies may apply to actions by a system, by management procedures, by employees, by system users.
  - A complete security policy is a collection policies on specific security issues.

NYU

Week 4

Examples of Policy Areas

- Protection of Sensitive Information
  - Addresses the protection goals
  - Defines the way people interact with the data (who gets access, discussing information, printing, storing, etc.)
  - Policy *may* prescribe the technology used to handle sensitive information (e. g., DoD)--this technology is one of the enforcement mechanisms
  - Audit is usually another enforcement mechanism
- Acceptable Use Policy for employee internet access on corporate systems
  - Defines what employees can and cannot use the corporate systems for on the Internet.
  - Should define penalties for violations
  - Enforcement: website blocking, activity logging and audit, individual workstation audit

NYU

Week 4

CS Dept Security Policy: Measures

These are some of the measures listed in the policy. Why are they needed? What properties does this influence?

- Throttle repeated unsuccessful login-attempts, rather than account lockout

NYU

Week 4

CS Dept Security Policy: Measures

These are some of the measures listed in the policy. Why are they needed? What properties does this influence?

- Throttle repeated unsuccessful login-attempts, rather than account lockout

  Availability

NYU

Week 4

CS Dept Security Policy: Measures

These are some of the measures listed in the policy. Why are they needed? What properties does this influence?

- Audit even successful login-attempts

Week 4

CS Dept Security Policy: Measures

These are some of the measures listed in the policy. Why are they needed? What properties does this influence?

- Audit even successful login-attempts

  Non-repudiation

Week 4

CS Dept Security Policy: Measures

These are some of the measures listed in the policy. Why are they needed? What properties does this influence?

- Disable default accounts and passwords on systems

Week 4

CS Dept Security Policy: Measures

These are some of the measures listed in the policy. Why are they needed? What properties does this influence?

- Disable default accounts and passwords on systems

  Access Control

Week 4

CS Dept Security Policy: Measures

These are some of the measures listed in the policy. Why are they needed? What properties does this influence?

- Maintain detailed documentation of everything

NYU

Week 4

CS Dept Security Policy: Measures

These are some of the measures listed in the policy. Why are they needed? What properties does this influence?

- Maintain detailed documentation of everything

  Non-repudiation, Accountability

Week 4

CS Dept Security Policy: Measures

These are some of the measures listed in the policy. Why are they needed? What properties does this influence?

- Write audit events to a separate system

Week 4

CS Dept Security Policy: Measures

These are some of the measures listed in the policy. Why are they needed? What properties does this influence?

- Write audit events to a separate system

  Availability, Non-repudiation

Week 4

CS Dept Security Policy: Measures

These are some of the measures listed in the policy. Why are they needed? What properties does this influence?

- Host based and Network based firewall

NYU

Week 4

CS Dept Security Policy: Measures

These are some of the measures listed in the policy. Why are they needed? What properties does this influence?

- Host based and Network based firewall

  Access Control

NYU

Week 4

CS Dept Security Policy: Measures

These are some of the measures listed in the policy. Why are they needed? What properties does this influence?

- Enable full disk encryption on portable devices, in addition to file/database encryption

Week 4

CS Dept Security Policy: Measures

These are some of the measures listed in the policy. Why are they needed? What properties does this influence?

- Enable full disk encryption on portable devices, in addition to file/database encryption

  Confidentiality, Privacy

Week 4

CS Dept Security Policy: Measures

These are some of the measures listed in the policy. Why are they needed? What properties does this influence?

- Destroy files as soon as they are no longer needed using approved methods

NYU

Week 4

CS Dept Security Policy: Measures

These are some of the measures listed in the policy. Why are they needed? What properties does this influence?

- Destroy files as soon as they are no longer needed using approved methods

Confidentiality

Week 4

What is the Basis for Most Security Policies?

- Broader organizational, corporate or government policies
- Risk analysis:
  - Often qualitative (even intuitive) analysis
  - Usually only based on analysis of assets at risk and threats
    - Sensitivity of data (both confidentiality and integrity) is a major source for many organizational level policies, which are based on classes of information (e. g., secret, proprietary, SSN, personal medical, etc.)
  - Vulnerabilities may drive lower level policy
- Concerns about image (corporate, agency, personal)

NYU

Week 4

Security Policy: General Principles

- Security policies are detailed, written documents
  - There are usually multiple documents describing policy on specific areas; e. g., “Internet usage by employees”, “Security patch installation policy”, “Password selection and handling policy” etc.
- Top level policies are often determined by management with significant input from IT: they represent the agency or corporate goals and principles
- It is important that the policies be distributed to those who have to follow the policy and/or implement the policy enforcement method.
- It is critical that employees be made aware of policies
  - It is recommended this is documented
- To be effective, a policy should have an enforcement mechanism

Week 4

Basic Policy Requirements for Employee Policies

Basic Policy Requirements

- Policies must:
  - be implementable and enforceable
  - be concise and easy to understand
  - balance protection with productivity
- Policies should:
  - state reasons why policy is needed
  - describe what is covered by the policies
  - define contacts and responsibilities
  - discuss how violations will be handled

NYU

Week 4

Who Should Be Concerned About Security Policy

- Managers
- System designers
- Users: what are the policy's impacts on their actions, and what are the ramifications of not following policy
- System administrators, support personnel who manage enforcement technologies and processes
- Company lawyers: they may have to use the written policies in support of actions taken against employees in violation

Week 4

Inclusive versus Exclusive Policies

- Inclusive policies explicitly state what is allowed, and all other actions are prohibited
  - “Employees may only use the Internet from corporate systems for business related email and web browsing”
  - “Employees may only use the Internet from corporate systems for business related email and web browsing. Occasional personal email and browsing are permitted as long as it does not impact employee performance, corporate system performance and does not include any pornography, illegal activities, or other materials detrimental to the corporation or its perception by the public”
- Exclusive policies explicitly state what is prohibited
  - “Employees may not use email or web browsers from corporate systems for personal use.”
  - “Employees may not use email or web browsers from corporate systems for pornography, illegal activities or other materials detrimental to the corporation or its perception by the public”

Week 4

Inclusive versus Exclusive Policies (continued)

- Inclusive policies provide automatic prohibition for new applications, technologies, (some) attacks, etc. without changing policy
  - Downloading copyright material for personal use
  - Instant Messaging
- Inclusive policies may need to be updated and updates distributed whenever a new application, technology, etc. comes along
- It is a matter of (high level) corporate policy whether to use inclusive or exclusive policies

NYU

Week 4

Examples of Policy Areas

- Employee email usage
- Employee web browsing usage
- Privacy of user information
- Password selection and protection
- Handling of proprietary information
- Cryptographic policy (what needs to be encrypted, what algorithms/implementations/key lengths to use)
- Remote Access
- Protection of employee issued laptops (physical and network connections)

Week 4

Examples of Policy Areas--System Management

- Configuration Management
- Ongoing Security Monitoring
- Security Patch Management
- Incident Response
- Business Continuity
- Security Audit

NYU

Week 4

Security Policies are at Multiple Levels

- High level policies are “human readable”
- High level policies are often at an organizational level and apply to all systems
- High level policies may be refined into multiple low-level policies that are apply to system actions, management processes, and actions by employees/users
  - For example, a top-level policy on protection of sensitive information may include lower level policies on access control lists (system actions), determining the sensitivity level of information (management processes), and who an employee may discuss the information with (employee actions)
  - Lower level policies may be specific to individual systems

Week 4

Security Policies are at Multiple Levels (continued)

- Multiple levels of a policy may be in a single document, but the development of the complete policy is “top down”
- This refinement process level policies may be integrated into the system design process
  - For example, you cannot define a firewall policy until you know your system will use a firewall as enforcement mechanism for a higher-level policy
- “High level” and “lower level” policy is not a standard terminology--this is a useful just a way to think about policies
- Some authors only consider the high-level policies as “policies”

Week 4

Example of Hierarchical Policies

- High level: "company proprietary information shall be protected from release to unauthorized personnel”
- Mid level procedural policy:
  - All proprietary information shall have a committee responsible for its control
  - A member must authorize any distribution of material
  - Enforcement: training, audit
- Mid level technology policy:
  - Proprietary information may only be stored on protected systems, accessible only to those with authorized access There shall be no externally initiated, automated means to retrieve information from the protected systems
    - Low level; e. g., a firewall rule blocking incoming traffic on ports 20 (ftp data), 21 (ftp control), and 69 (tftp)
    - The firewall is the enforcement mechanism

Week 4

Security Policies and Systems Engineering

- Top level policies are usually at an organizational, not system level
  - Such policies typically exist before a system development process begins
  - They reflect general organizational policies and goals, such as the handling of classes of sensitive data used broadly in the organization, not just in a single system
  - Top level policies lead to top level system requirements in the initial requirements phase
  - All organizational policies should be reviewed for relevancy at the start of the systems engineering process

Week 4

Security Policies and Systems Engineering (continued)

- At the start of the system design process proceeds, the top-level policies may impact the requirements (and hence architecture and design)
- As the system design process proceeds, the architecture of the system will lead to system specific policy interpretations of the top level policy, the “system policy”
- The system policy in turn is an input into the system and security design
- This may be iterated (depending on the systems engineering model used), with policy refinements occurring as the design is refined
  - At what point does this become requirements allocation and not policy refinement? There is no set rule…
- Conformance with policy is part of the assessment at each iteration

Week 4

Source of Sample Policy Documents and Information

- The SANS (SysAdmin, Audit, Network, Security) Institute has sample security policies available on-line in many areas. These can be downloaded and used as is, or modified to the needs of a specific company
  - http://www.sans.org/resources/policies/
- IETF Site Security Handbook (policies for systems admins)
  - https://www.rfc-editor.org/info/rfc2196
- NIST web site: lots of material on security: technology, best practices, policies, regulations, etc. A search for “security policy” on that site got 6090 hits
  - csrc.nist.gov

Week 4

PCI Policies

- Top Level: Credit card information should not be disclosed
  - Mid level: All PCI networks and systems will be protected against “snooping” by unauthorized entities
  - The PCI system shall not permit clerks or other customers to see PIN numbers as they are entered by customers
- Top Level: The PCI system shall not violate the integrity of the authorization process
  - Mid Level: Clerks shall not override a “no” response to a credit authorization request
    - Lower Level: The PCI system shall automatically block completion of a transaction that has been denied

      (or)
    - Clerk shall be trained to never complete a transaction that has been denied

(In practice policies would be more detailed and have more elements)

Week 4

Windows 10 Privacy Concerns

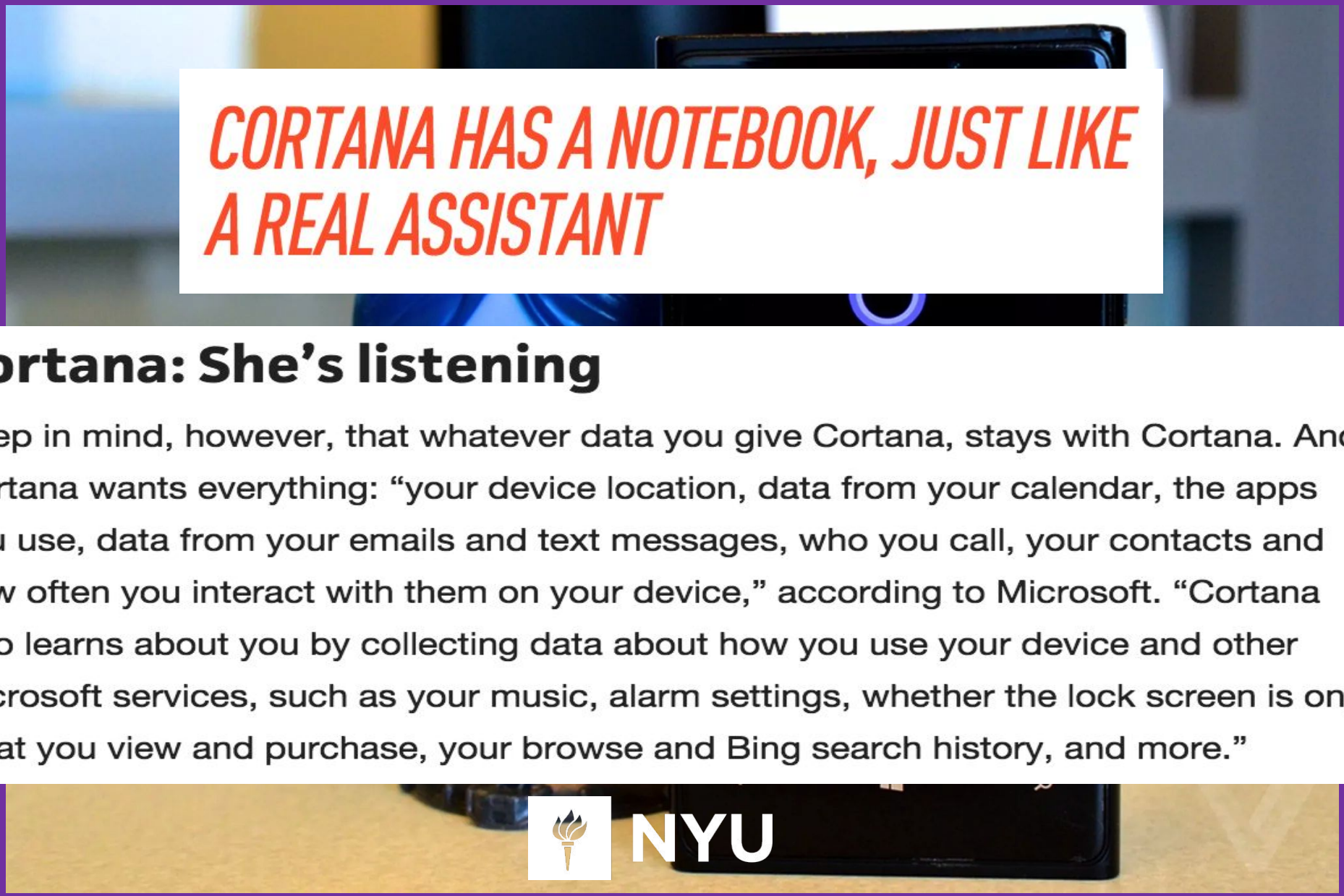
- Default setting is to sync all data and settings to Microsoft's servers
- Profiles Windows usage
- Same policy applies to all data, whether stored locally on the machine or on the cloud.

> Rather than residing as a static software program on your device, key components of Windows are cloud-based. ... In order to provide this computing experience, we collect data about you, your device, and the way you use Windows.

In other words, Microsoft won't treat your local data with any more privacy than it treats your data on its servers and may upload your local data to its servers arbitrarily —unless you stop Microsoft from doing so. Microsoft's security story has been far from perfect; this move could make it far worse. For now, it's not easy to restrict what

Week 4

Meet Cortana



Cortana: She's listening

Keep in mind, however, that whatever data you give Cortana, stays with Cortana. And Cortana wants everything: "your device location, data from your calendar, the apps you use, data from your emails and text messages, who you call, your contacts and how often you interact with them on your device," according to Microsoft. "Cortana also learns about you by collecting data about how you use your device and other Microsoft services, such as your music, alarm settings, whether the lock screen is on, what you view and purchase, your browse and Bing search history, and more."

NYU

Week 4

Privacy Policy Q/A

Microsoft collects bug reports from users when an application crashes.

- Does personally identifiable information make its way into the crash reports sent to Microsoft?

NYU

Week 4

Privacy Policy Q/A

Microsoft collects bug reports from users when an application crashes.

- Does personally identifiable information make its way into the crash reports sent to Microsoft?

Yes.

Is this reasonable?

Week 4

Privacy Policy Q/A

- Do you think Microsoft is sent every picture you take that is stored on your computer's local hard drive?

Week 4

Privacy Policy Q/A

- Do you think Microsoft is sent every picture you take that is stored on your computer's local hard drive?

No.

This seems like it would be a clear privacy violation.

NYU

Week 4

Privacy Policy Q/A

- Does Microsoft know what websites are currently open on your browser?

Week 4

Privacy Policy Q/A

- Does Microsoft know what websites are currently open on your browser?

Yes.

This is done to offer a personalized web browsing experience.

Is this reasonable?

NYU

Week 4

Privacy Policy Q/A

- Do you think Microsoft collects your Wi-Fi password and shares it with others?

NYU

Week 4

Privacy Policy Q/A

- Do you think Microsoft collects your Wi-Fi password and shares it with others?

  Yes.

Microsoft collects your Wi-Fi password and shares it with your contacts by default. This lets people connect automatically.

Is this reasonable?

NYU

Week 4

Has Microsoft Gone Too Far?

Underground Piracy Sites Want To Block Windows 10 Users

394

Posted by **timothy** on Sunday August 23, 2015 @08:30AM from the so-cool-to-be-underground-like-Windows-7 dept.

An anonymous reader writes:

> Some smaller pirate sites have become concerned about Windows 10 system phoning home too many hints regarding that the users are accessing their site. Therefore, the pirate administrators have started blocking Windows 10 users from accessing the BitTorrent trackers that the sites host. The first ones to hit the alarm button were iTS, which have posted a statement and started redirecting Windows 10 users to a YouTube video called Windows 10 is a Tool to Spy on Everything You Do. Additionally, according to TorrentFreak, two other similar dark web torrent trackers are also considering following suit. "As we all know, Microsoft recently released Windows 10. You as a member should know, that we as a site are thinking about banning the OS from FSC," said one of the FSC staff. Likewise, in a message to their users, a BB admin said something similar: "We have also found [Windows 10] will be gathering information on users' P2P use to be shared with anti piracy group."

Windows 10's Privacy Policy: the New Normal?

515

Posted by **Soulskill** on Saturday August 08, 2015 @08:05PM from the no-i-do-not-want-to-send-a-crash-report dept.

An anonymous reader writes:

> The launch of Windows 10 brought a lot of users kicking and screaming to the "connected desktop." Its benefits come with tradeoffs: "the online service providers can track which devices are making which requests, which devices are near which Wi-Fi networks, and feasibly might be able to track how devices move around. The service providers will all claim that the data is anonymized, and that no persistent tracking is performed... but it almost certainly could be." There are non-trivial privacy concerns, particularly for default settings.
>
> According to Peter Bright, for better or worse this is the new normal for mainstream operating systems. We're going to have to either get used to it, or get used to fighting with settings to turn it all off. "The days of mainstream operating systems that don't integrate cloud services, that don't exploit machine learning and big data, that don't let developers know which features are used and what problems occur, are behind us, and they're not coming back. This may cost us some amount of privacy, but we'll tend to get something in return: software that can do more things and that works better."

Week 4

How Much Privacy Can You Really Have?

Windows 10 sends identifiable data to Microsoft despite privacy settings

Operating system contacts OneDrive, MSN and other services even if a user has activated privacy-protecting options, report discovers

Windows 10 sends identifiable information to Microsoft, even if a user turns off its Bing search and Cortana features, and activates the software's privacy-protection settings.

How To Keep Mi

418

Posted by samzenp

MojoKid writes:

> Amid the privacy c
> how to minimize le
> are using Windows
> the installation/upg
> accessed via the S
> options regarding
> re

on
If you
ing
n be
of
s OS

Windows Telemetry Rolls Out

469

Posted by **samzenpus** on Monday September 07, 2015 @03:13PM from the here-it-comes dept.

ihtoit writes:

> Last week came the warning, now comes the roll out. One of the most most controversial aspects of Windows 10 is coming to Windows 7 and 8. Microsoft has released upgrades which enable the company to track what a user is doing. The updates – KB3075249, KB3080149 and KB3068708 – all add "customer experience and diagnostic telemetry" to the older versions. gHacks points out that the updates will ignore any previous user preferences reporting: "These four updates ignore existing user preferences stored in Windows 7 and Windows 8 (including any edits made to the Hosts file) and immediately starts exchanging user data with vortex-win.data.microsoft.com and settings-win.data.microsoft.com."

NYU

A General Question

- Given a computer system, how can we determine if it is secure? More simply, is there a generic algorithm that allows us to determine whether a computer system is secure?
- What policy shall define “secure?” For a general result, the definition should be as broad as possible – access control matrix with some basic operations and commands.

Week 4

Exam 1

Exam 1 next week!

Start learning Python / RePy

Python tutorial: http://docs.python.org/tutorial/

Seattle tutorials: https://github.com/paoga87/r2py-assignment-docs/blob/master/Programming/RepyV2API.md

Week 4

Reading Next Week

Read through the TSA policies for travel:
https://www.tsa.gov/travel/security-screening/whatcanibring/all

Why / how does this work?
http://www.dubfire.net/boarding_pass/

Why bike theft pays...
https://www.bloomberg.com/news/articles/2012-09-14/why-bike-theft-is-so-hard-to-stop
... and bank robbery does not
https://www.wsj.com/articles/BL-IMB-3561

Purpose: Think about how policies impact attack trees!

NYU

Week 4

What will be on Exam 1

Open note – no devices!

Core items to know:

- How to think like an attacker
  - "What could possibly go wrong?"
- Ethics
- Attack trees / risk
- Mechanism vs policy
- Intuition behind the security design principles, BLP, Biba