


Introduction and Principles of Computer Security

Royal Mail's recovery from ransomware attack will cost business at least \$12M

First time hard figure given on recovery costs for January incident

 [Connor Jones](#)

Casino giant Caesars tells thousands: Yup, ransomware crooks stole your data

House always wins, er, wait ...

[T-MOBILE](#) / [MOBILE](#) / [TECH](#)

T-Mobile discloses its second data breach so far this year




/ A hacker gained access to the personal information of hundreds of T-Mobile customers between February and March.

City of Oakland declares state of emergency after ransomware attack

By [Sergiu Gatlan](#)

 February 15, 2023

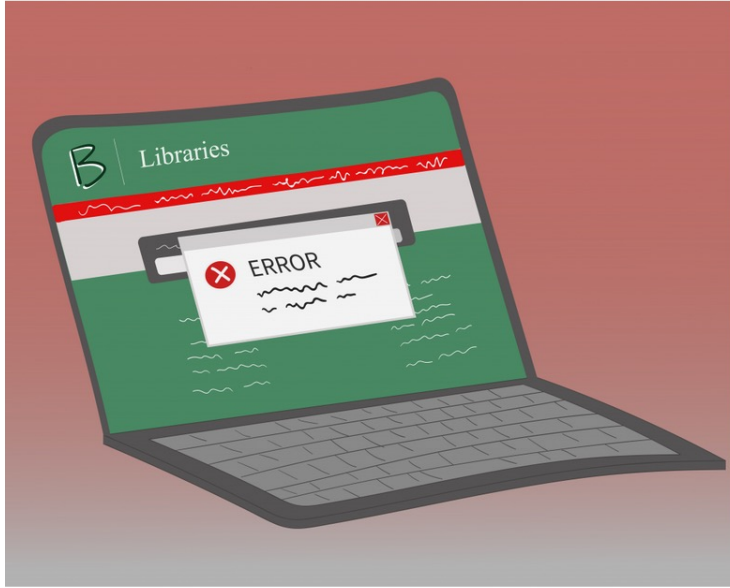
 10:47 AM

 3

We are victims

CAMPUS NEWS

University fallen victim to cybersecurity breach



Jordan Skube/Design Manager

During the weekend of Nov. 7 2020, computer servers at Binghamton University became the target of “malicious activity” according to the University’s website, resulting in some services going offline.

Information Technology Task Force security recommendations approved

Implementation of two-factor authentication to begin mid-month

2FA
TWO-FACTOR AUTHENTICATION

What is Computer Security?

- **Security:** the state of being free from danger or threat
 - National security, financial security...
- **Information security:** information is free from danger or threat of an **adversary**
- **Computer security (cyber security):** information security as applied to computing devices
 - Involves **adversary(attacker, hacker)** who is active and malicious

Information Security Principles

- **Confidentiality**: the secrecy of information
- **Integrity**: the accuracy and consistency of information over its entire life-cycle
- **Availability**: the ability to use the information desired

“CIA”, but don’t get confused with this
CIA



Confidentiality

- The secrecy of information
- Preventing the unauthorized *reading* of information
 - Corporate secrets
 - Personal sensitive information

Integrity

- The accuracy and consistency of information over its entire life-cycle
- Detecting/Preventing unauthorized *writing(change)* of information
 - Destroy/Change records
 - Installs unwanted software(spyware, malware, etc.)

Availability

- The ability to use the information desired
- Related to the reliability and system design
- Data is available in a *timely manner* when needed
 - Attacker deliberately arrange to deny access to data or service by making it unavailable
- The attempts to block availability is called **Denial of Service(DOS) attacks**
 - Flooding messages to a target system that force it to shut down

Besides CIA

- **Authenticity:** the truthfulness of an attribute of a single piece of data or entity
 - Authentication: the act of enforcing authenticity
 - Prove who you are
- **Non-repudiation:** the purported maker of a statement will not be able to successfully challenge its validity
 - Person cannot deny the authenticity of their signature on document
- **Accountability:** every individual who works with an information system should have specific responsibilities for information assurance
 - Activities can be traced to individual

Principles of information security

- Confidentiality
- Integrity
- Availability
- Authenticity
- Accountability
- Non-repudiation

Buy 10 books from Amazon with credit card



- Confidentiality
- Integrity
- Availability
- Authenticity
- Accountability
- Non-repudiation

Amazon.com must be online



amazon.com®

 citibank®

Availability

- Confidentiality
- Integrity
- **Availability**
- Authenticity
- Accountability
- Non-repudiation

User logs into Amazon.com



Password



Authenticity

- Confidentiality
- Integrity
- Availability
- **Authenticity**
- Accountability
- Non-repudiation

Password shouldn't be in plaintext

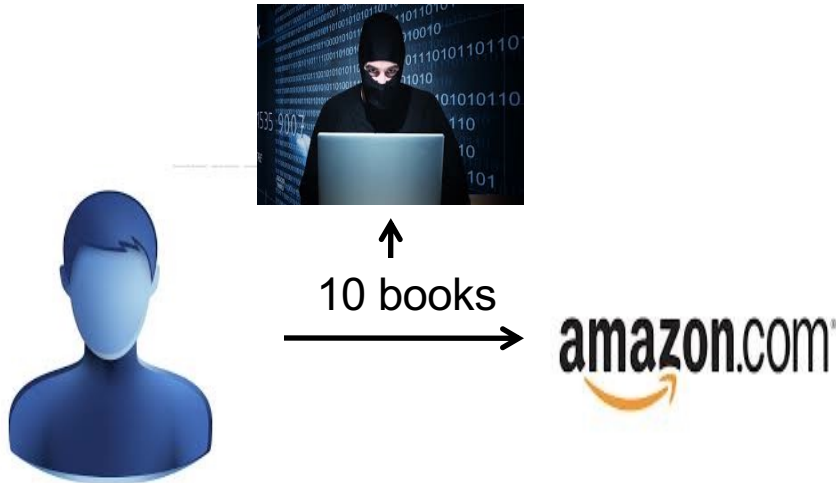


Confidentiality



- **Confidentiality**
- Integrity
- Availability
- Authenticity
- Accountability
- Non-repudiation

The hacker can't change 10 → 100



Integrity



- Confidentiality
- **Integrity**
- Availability
- Authenticity
- Accountability
- Non-repudiation

Credit card shouldn't be in plaintext



citibank[®]

Confidentiality

- **Confidentiality**
- Integrity
- Availability
- Authenticity
- Accountability
- Non-repudiation

Citibank must be online



Availability

- Confidentiality
- Integrity
- **Availability**
- Authenticity
- Accountability
- Non-repudiation

Citibank verifies the request from Amazon



amazon.com®

Hooray, I am Amazon!



citibank®

Authenticity

- Confidentiality
- Integrity
- Availability
- **Authenticity**
- Accountability
- Non-repudiation

Amazon verifies this is indeed Citibank



amazon.com®

Hooray, I am Amazon!



citibank®

Hooray, I am Citibank!

Authenticity

- Confidentiality
- Integrity
- Availability
- **Authenticity**
- Accountability
- Non-repudiation

Credit card, again, shouldn't be in plaintext



Confidentiality

- Confidentiality
- Integrity
- Availability
- Authenticity
- Accountability
- Non-repudiation

Citibank verifies user information



Authenticity

- Confidentiality
- Integrity
- Availability
- **Authenticity**
- Accountability
- Non-repudiation

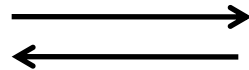
Charge amount shouldn't be changed



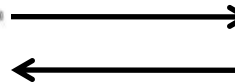
Integrity

- Confidentiality
- **Integrity**
- Availability
- Authenticity
- Accountability
- Non-repudiation

Amazon asks some worker to ship 10 books to the user



amazon.com[®]



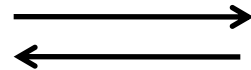


Where are the books?

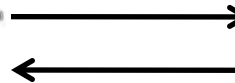
Accountability

- Confidentiality
- Integrity
- Availability
- Authenticity
- **Accountability**
- Non-repudiation

Amazon should make sure that the user can't repudiate the transaction later



amazon.com[®]



citibank[®]

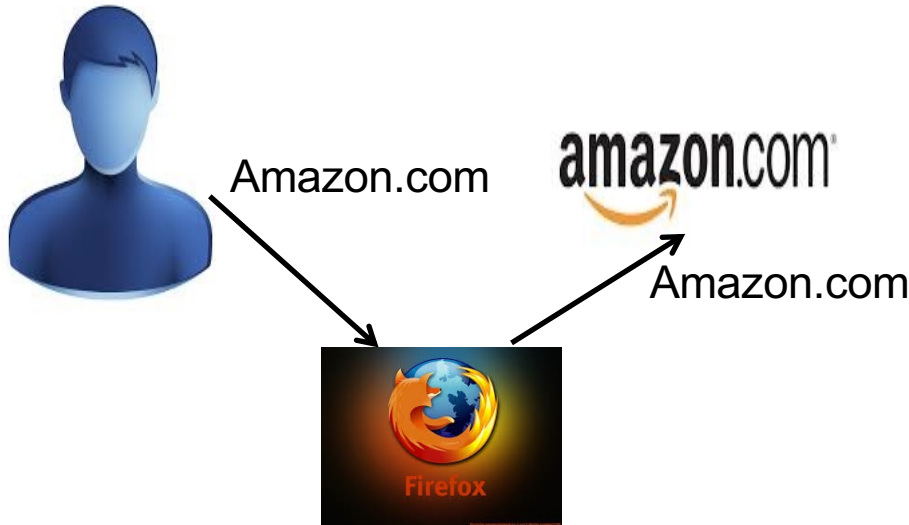
Non-Repudiation

- Confidentiality
- Integrity
- Availability
- Authenticity
- Accountability
- **Non-repudiation**

Challenges in a paranoid world

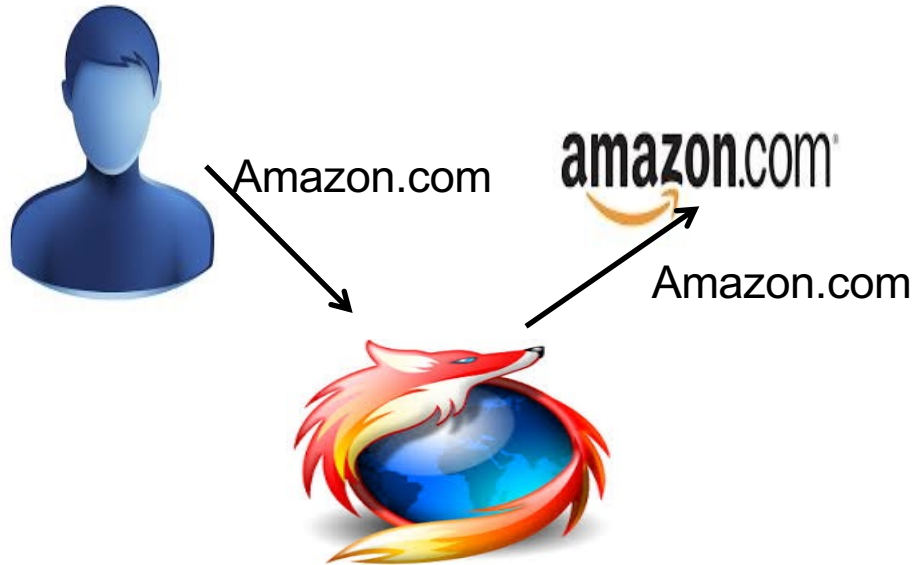


How does the user know that he has indeed logged into Amazon.com?



User **trusts** browser

What if the browser is bad?



citibank[®]

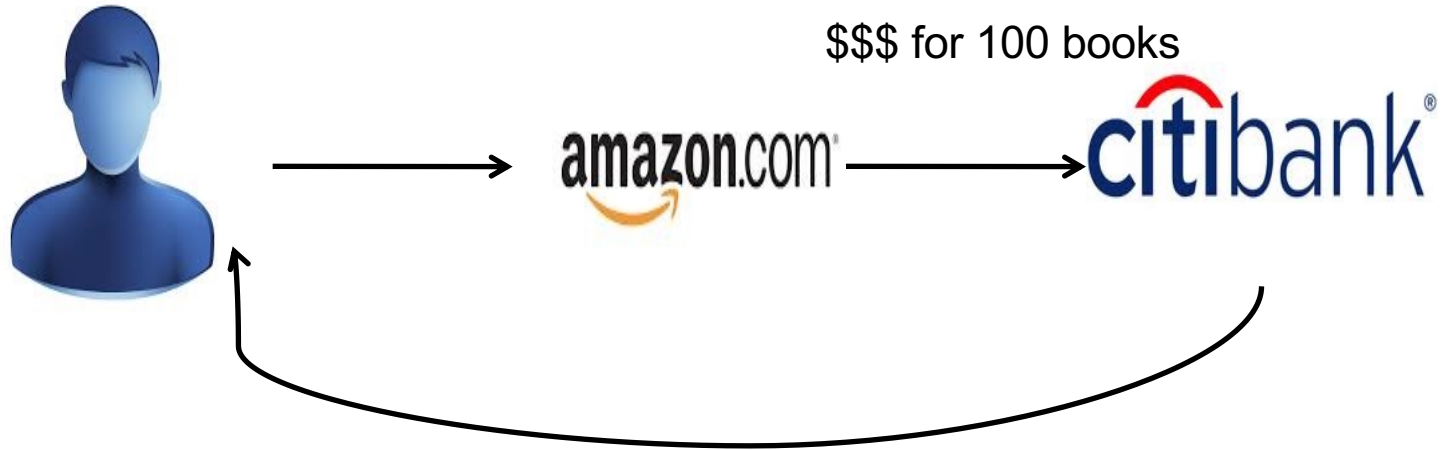
The **bad** browser can remember user's password, transactions info

How does the user know that Amazon will only request the charge for 10 books?



The user **trusts** Amazon

What if Amazon is dishonest?



User verifies monthly bill from Citibank
and catches the error; there is a chance
that you missed it 😞

How does the user know the credit card information stored at Amazon.com is safe?



The user **trusts** that Amazon.com is safe

How does the user know no one is trying to figure out his password at Amazon.com?



The user **trusts** that his password is not guessable

Challenges in a paranoid world



Including ourselves

Human errors key in computer security

- Human errors contribute to 95% of the cyber security incidents worldwide
 - @lanl.gov → @lanl.govv; @lanl.gov → @lanl.goov
 - www.amazon.com → www.amazoon.com
- Which one is correct?
 - A: www.binghamtom.edu
 - B: www.binghantom.edu
 - C: www.binghanton.edu
 - D: www.bighamton.edu
 - E: www.binghamton.edu
 - F: www.binghamtone.edu

Social engineering

- **Social engineering** in computer security: psychological manipulation of human beings into performing certain actions or divulging confidential information
- **Phishing email attack:** an email that appears from a legitimate entity requesting, directly or indirectly, certain private information, such as PII (Personal Identifiable Information), credit card number, and banking information.

Snapshot of phishing scam



INFORMATION SUPPORT SERVICES <talktoalexrn@gmail.com>

to bcc: me ▼

The services of students are urgently required to work as Research Assistants and get paid **\$400** weekly. Tasks given are very easy and are being done remotely. This position is open to all students of **BINGHAMTON UNIVERSITY** regardless of your department.

For more information submit your full name, functional cell phone number, year of study and Department via this email or text **Prof** on (408) 800-2136.

Sincerely,

Prof.

Distinguished Professor

Center Director.

Department of Computer Science.

How to ensure principles of computer security?

Cryptography

Access Control

Security Protocols

System Security

How to achieve computer security?

- Be able to eliminate bugs and design flaws and/or make them **harder to exploit**
- **Be able to think like attackers**
 - A police detective...
 - ...must study and understand criminals
- Develop a foundation for **deeply understanding** the systems we use and build

Broader Issues: Ethics, Law, Privacy

Definition of Ethics

- Ethics: “The science of morals; the department of study concerned with the principles of human duty. The moral principles by which a person is guided.”

– Oxford English Dictionary

Ethics in Computer Security

- **Ethics in Computer Security:** guide the professional behavior of those who have access to information systems
 - E.g., Access the client information in the database
- Respect for privacy
 - Respect confidential information and the potential consequences of violating privacy
- **Why Ethics Matter in computer security**
 - Trust: Computer security professionals are trusted with sensitive data and powerful tools. Have *authorized* access.

What is a hacker?

- Hacker

“A person with an enthusiasm for programming or using computers as an end in itself.”

Or, “A person who uses his skill with computers to try to gain unauthorized access to computer files or networks.”

– Oxford English Dictionary

- The term is misleading

- **Self-described hackers** – enjoy experimenting with technology and writing code
- **Media-labeled hackers (crackers, attackers)** – break into systems, cause damage, and write malware, ransomware
- **Ethical hackers** – former hackers or crackers who have joined the security industry to test network security and create security products and services

Goodies or Baddies?

- **Black Hats**

- Break into systems, develop and share vulnerabilities, exploits, malicious code, and attack tools

- **White Hats**

- Are part of the “security community,” help find security flaws, but share them with vendors so that products can be made safer

- **Grey Hats**

- Some in between



Black Hats Hacking is Unethical

- Causes harm
- Denies access to resources or services
- Violates property and privacy rights
- Allows for no control or accountability
- Difference between criminal hackers and script kiddies – intent to **profit**



Suppose you find a bug...

- Publishing details of software vulnerabilities and exploits – sometimes before vendors are given a chance to fix them
- **Reasons for disclosing it**
 - Helps researchers understand technologies and flaws, furthers knowledge
 - Helps make products more secure
- **Reasons for not disclosing it**
 - Information can be used by hackers to attack systems or write malware
 - Makes the Internet less secure
- **Full disclosure guidelines**
 - 30-day period to allow vendors to develop patches
 - Need for vendor responsiveness

Software Vendor Responsibility

- Thousands of software vulnerabilities discovered every year
- Puts users at risk
- Minimum secure programming standards
- Security vs. functionality
 - Vendor usually choose functionality over security
 - **Should security be a priority?**
- Legal liability for computer software security – like other industries

Cyberlaw - Difficulties

- Internet still relatively “lawless”
- Cyberlaw is constantly changing, evolving, being shaped through experience
- Internet doesn't fit into traditional notions of territoriality and state boundaries
- The Internet creates jurisdictional challenges
- Uniform laws don't exist everywhere



Jurisdiction Challenges

- **Responsibility**

- No single entity governs the Internet
- Responsibility is shared among states, nation-states, and international entities

- **Standards Bodies**

- Entities like ICANN and NANOG develop standards but don't enforce laws

- **Jurisdictional Issues**

- The *global* nature of the Internet raises complex questions about jurisdiction

- **Cybercrime Challenges**

- The difficulties in determining the hacker's location, server locations, and the path of data across borders

- **Legal Complexity**

- The "territorial" problem persists - the challenge of applying different national laws to a borderless digital realm

Law Enforcement

- **Insufficient reporting** (CSI/FBI report – only 30% of companies that experienced computer intrusions reported them to law enforcement)
- **Lacking cyber investigation and law enforcement skills and knowledge**
- **Lacking tools and technologies**



Privacy – The Growing Threat?

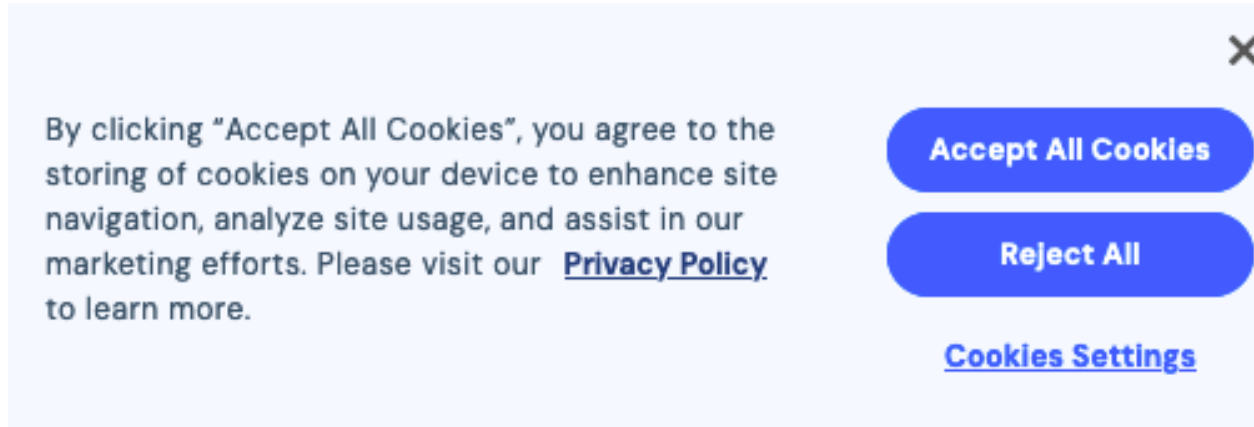
- Privacy: the power to control what other people know about you
- Big data era: a lot of data about you have been collected
 - You will be amazed by the information collected from the public domain solely



Privacy – The Growing Threat?

- What information is out there about you?
 - Financial data: credit history, mortgage, salary etc.
 - Interaction with government(s): SSN, driver's license, taxes, visa applications, criminal record.
 - Medical information: medical history, doctor's visits, medication, operations, health issues.
 - Communications data: landline and cell phone usage (including location!), e-mail messages, websites visited, online shopping.
 - Financial transactions: credit card transactions, purchases (often with details), deposits and withdrawals etc.
 - Travel details: places visited, means of transportation, routes etc.
 - Miscellaneous: All sorts of other info, including reading habits, hobbies etc.

Securing Privacy



- Implementation of privacy laws of the European Union's General Data Protection Regulation (GDPR)
 - Require websites to obtain user consent before collecting personal data, like Cookies

But...



I don't care about cookies

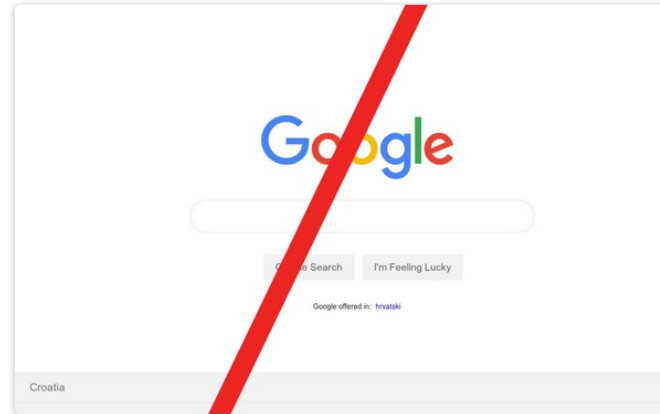
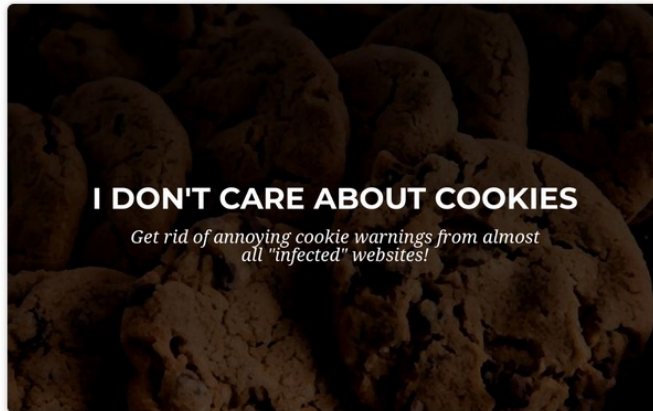
Add to Chrome

Featured 3.9★ (1.2K ratings)

Extension

Accessibility

900,000 users



Privacy vs. Security

- There has always been a delicate balance between privacy and security.
- Sept. 11, 2001 and the ongoing war on terrorism have forced a re-evaluation of the privacy vs. security balance

