ENEE 459-C
Computer Security

Introduction

UNIVERSITY OF
MARYLAND

Organization

- Class webpage
  - http://enee459c.github.io
  - Two lectures per week
  - Tuesday & Thursday 12.30 pm - 1.45 pm
  - PHY 1219
  - Attendance and participation is important
- My information
  - cpap at umd.edu
  - Office hours: Tuesday, 2pm-3pm, AVW 3409
- Teaching assistant
  - Sailunsi Chen
  - sailunsi at umd.edu
  - Office hours: TBA

Homeworks and lectures

- Final grade
  - 5 homeworks (40%)
  - Midterm (20%)
  - Final (30%)
  - Class attendance (10%)
- Lectures will be published on the webpage after class
- Homework and programming assignments will be published on the class webpage, but should be submitted through Canvas.
- No late homework submissions will be accepted
- Discussions will be managed at Canvas.

Prerequisites

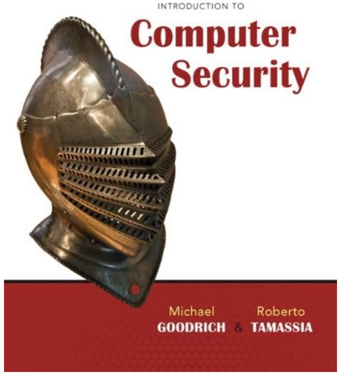
- ENEE150 or CMSC132
- The course will have a significant programming component
- Knowledge of algorithms and data structures is desirable

What is this course about?

- Introduction to Computer Security
  - Goals of Computer Security
  - Attacks
  - Defenses
- Fundamental concepts in Computer Security
  - Encryption
  - Integrity
  - Authentication
  - Access control
- Practical Computer Security
  - Web security
  - Cloud security
  - Network security
  - Systems and software security

Readings

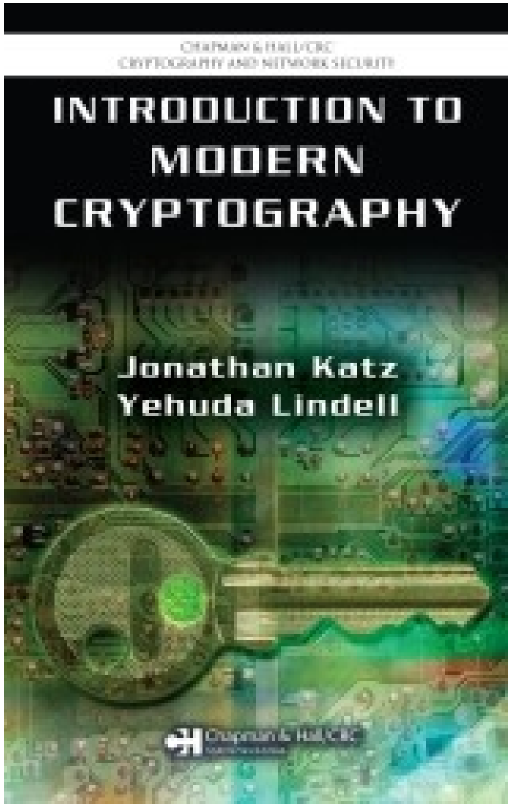
- Most of the class is based on the following textbook (GT

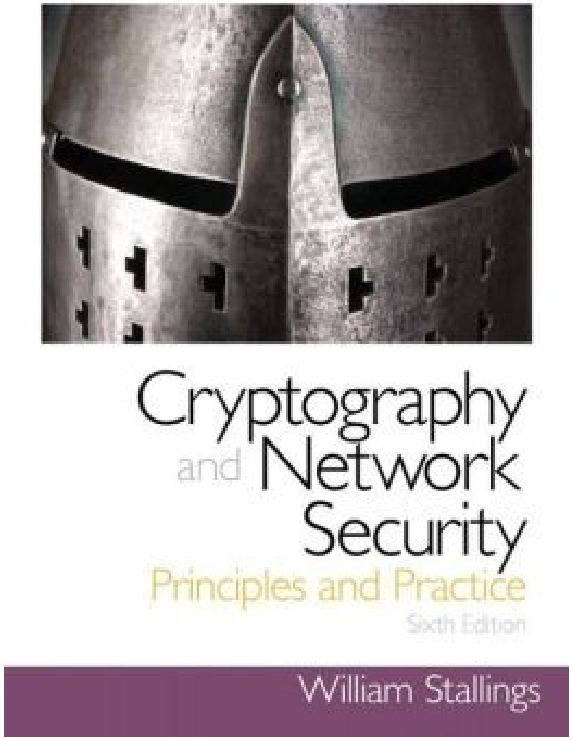


- Thanks to Michael Goodrich and Roberto Tamassia for making the content available
- We are going to be using the board too, so it is advisable you keep notes as well
- The library has copies of the book

Other readings

- Other recommended readings are (KL) and (WS)


CHAPMAN & HALL/CRC
CRYPTOGRAPHY AND NETWORK SECURITY
INTRODUCTION TO MODERN CRYPTOGRAPHY
Jonathan Katz
Yehuda Lindell
Chapman & Hall/CRC



What is Computer Security?

Computer Security

is the prevention of, or protection against

- access to information by unauthorized recipients
- intentional but unauthorized destruction or alteration of that information

Computer Security Goals

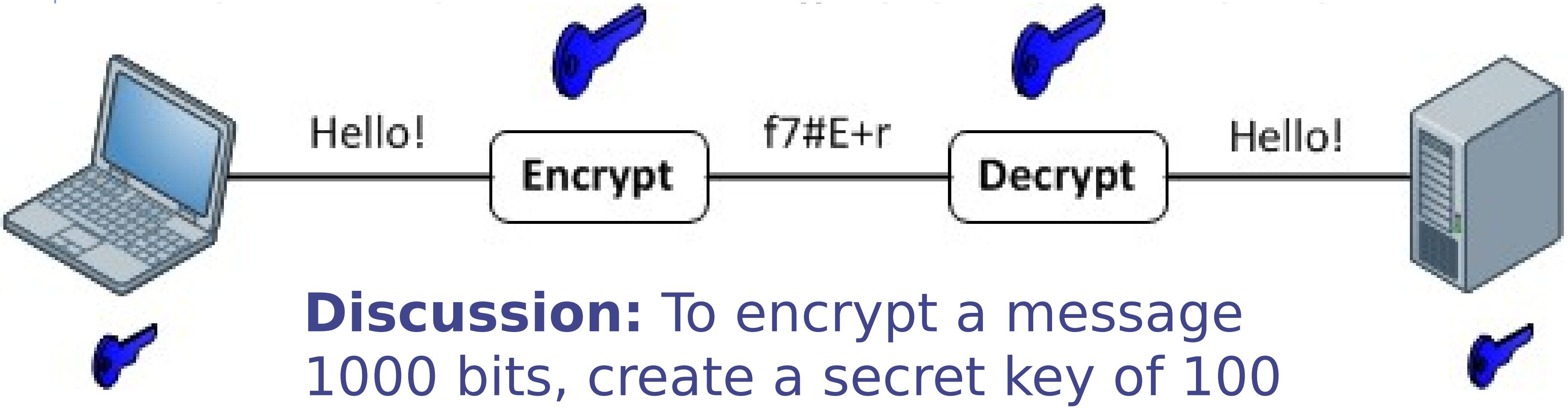
- Confidentiality
- Integrity
- Availability
- Authenticity
- Anonymity

Confidentiality

- It is the avoidance of the unauthorized disclosure of information
- It involves the protection of data, providing access for those who are allowed to see it while disallowing others from learning anything about its content
- E.g., nobody should be able to read the emails I am sending to my friends, except for my friends

Tools for confidentiality

- **Encryption:** the transformation of information using a secret, called an encryption key, so that the transformed information can only be read

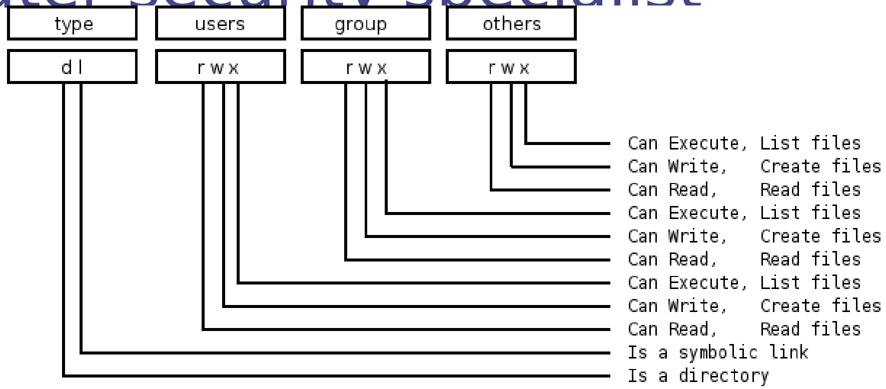


Discussion: To encrypt a message 1000 bits, create a secret key of 100 bits and XOR 100-bit blocks sequentially.

Does this reveal the content of the message?
Is this good enough?

Tools for confidentiality

- **Access control:** rules and policies that limit access to confidential information to those people and/or systems with a “need to know”
  - This need to know may be determined by identity, such as a person’s name or a computer’s serial number, or by a role that a person has, such as being a manager or a computer security specialist



Tools for confidentiality

- **Authentication:** the determination of the identity or role that someone has. This determination can be done in a number of different ways, but it is usually based on a combination of
  - **something the person has** (like a smart card or a radio key fob storing secret keys)
  - **something the person knows** (like a password)
  - **something the p** (like a human with a fingerprint)

Integrity

- The property that information has not be altered in an unauthorized way
- **Tools:**
  - **Checksums:** the computation of a function that maps the contents of a file to a numerical value. A checksum function depends on the entire contents of a file and is designed in a way that even a small change to the input file (such as flipping a single bit) is highly likely to result in a different output value.
  - **Discussion:** Can we use the checksum f(x) = x mod M?

Availability

- **Availability:** the property that information is accessible and modifiable in a timely fashion by those authorized to do so
- **Tools:**
  - **Physical protections:** infrastructure meant to keep information available even in the event of physical challenges.
  - **Computational redundancies:** computers and storage devices that serve as back-ups in the case of failures

Other important Security goals

- Authenticity

- Anonymity

Authenticity

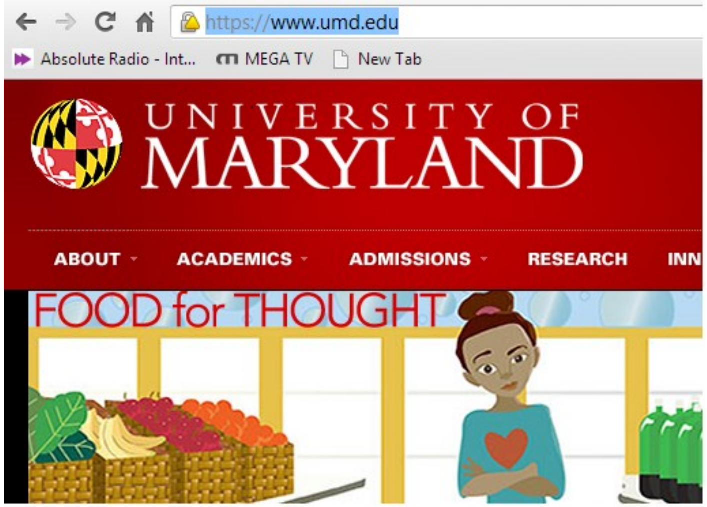
- **Authenticity** is the ability to determine that statements, policies, and permissions issued by persons or systems are genuine
- **Primary tool:**
  - **Digital signatures.** These are cryptographic computations that allow a person or system to commit to the authenticity of their documents in a unique way that achieves **nonrepudiation**, which is the property that authentic statements issued by some person or system cannot be denied

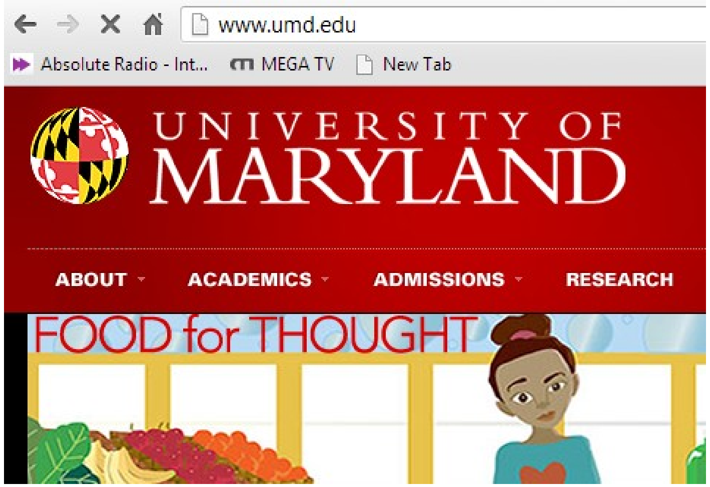
Anonymity

- **Anonymity:** the property that certain records or transactions not to be attributable to any individual
- **Tools:**
  - **Aggregation:** the combining of data from many individuals so that disclosed sums or averages cannot be tied to any individual
  - **Proxies:** trusted agents that are willing to engage in actions for an individual in a way that cannot be traced back to that person
  - **Pseudonyms:** fictional identities that can fill in for real identities in communications and transactions, but are otherwise known only to a trusted entity

Examples: HTTPS protocol

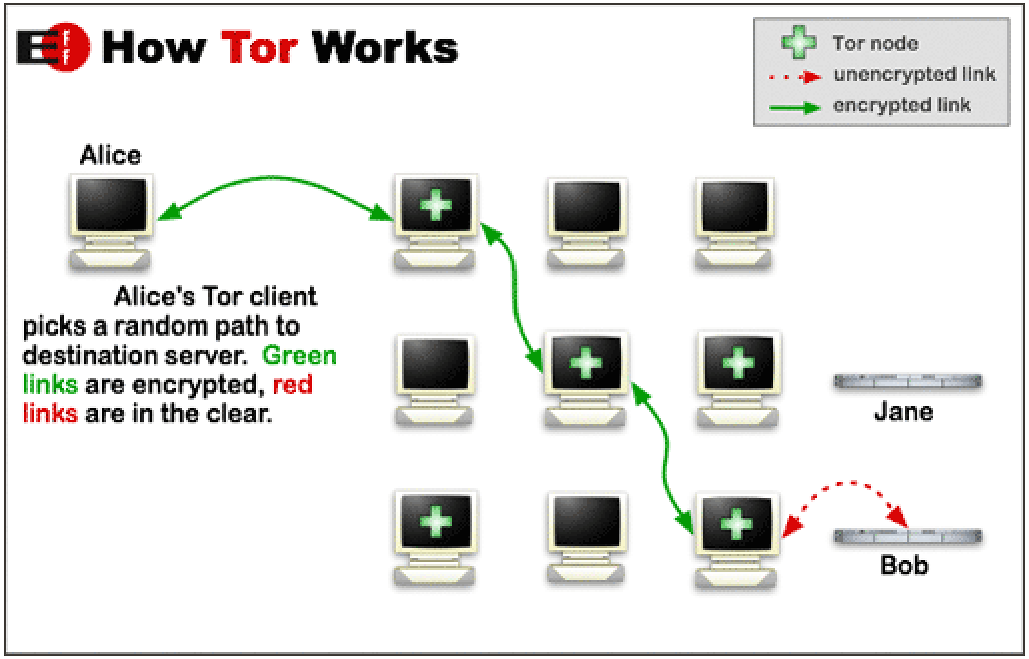
- Confidentiality
- Integrity
- Availability
- Authenticity
- Anonymity





Examples: TOR protocol

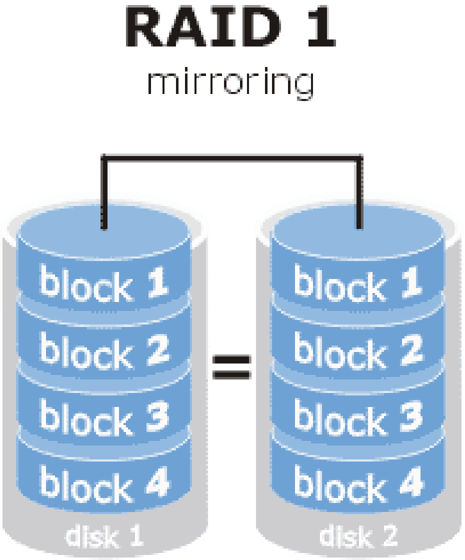
- Confidentiality
- Integrity
- Availability
- Authenticity
- Anonymity



Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

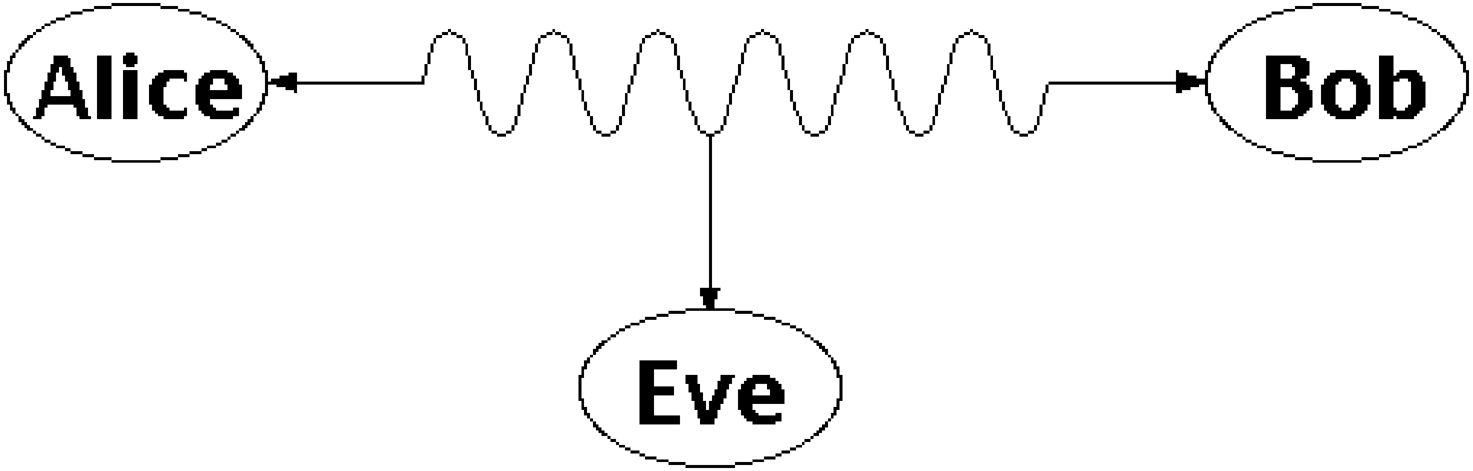
Examples: RAID technology

- Confidentiality
- Integrity
- Availability
- Authenticity
- Anonymity



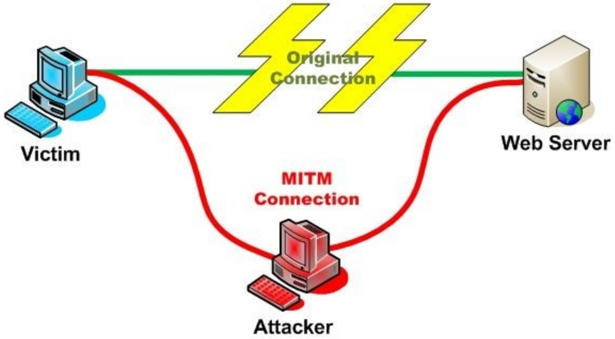
Threats and attacks

- **Eavesdropping:** the interception of information intended for someone else during its transmission over a communication channel



Threats and attacks

- **Alteration:** unauthorized modification of information
  - **Example:** the man-in-the-middle attack, where a network stream is intercepted, modified, and

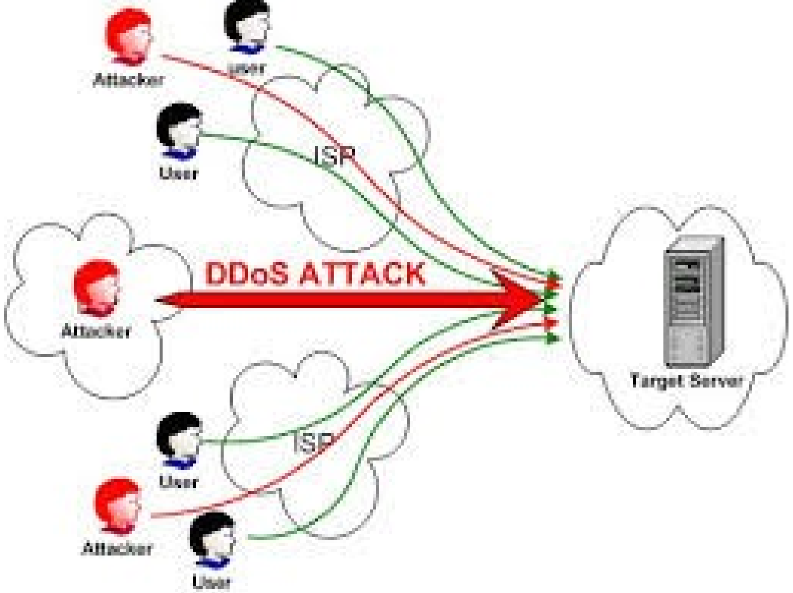


Threats and attacks

- **Software bugs:** Code is not doing what is supposed to be doing
  - **Example:** Some application code is mistakenly using an algorithm for encryption that has been broken

Threats and attacks

- **Denial-of-service:** the interruption or degradation of a data service or information access
  - **Example:** email **spam,** to the degree that it is meant to simply fill up a mail queue and slow down an email server



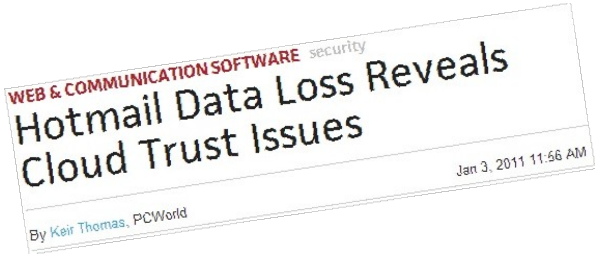
Threats and attacks

- **Masquerading**: the fabrication of information that is purported to be from someone who is not actually the author
- **Repudiation:** the denial of a commitment or data receipt.
  - This involves an attempt to back out of a contract or a protocol that requires the different parties to provide receipts acknowledging that data has been received

Threats and attacks

- **Correlation** and **traceback:** the integration of multiple data sources and information flows to determine the source of a particular data stream or piece of information

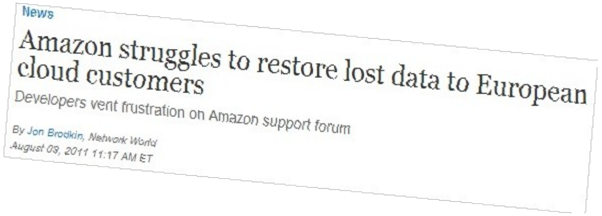
Attacks every day


WEB & COMMUNICATION SOFTWARE security

Hotmail Data Loss Reveals Cloud Trust Issues

Jan 3, 2011 11:56 AM

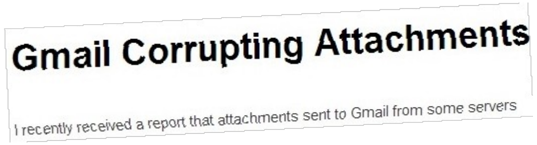
By Keir Thomas, PCWorld


News

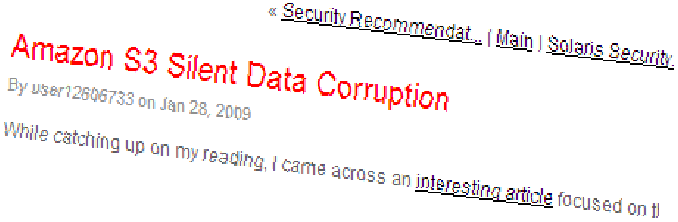
Amazon struggles to restore lost data to European cloud customers

Developers vent frustration on Amazon support forum

By Jon Brodkin, Network World
August 09, 2011 11:17 AM ET


Gmail Corrupting Attachments

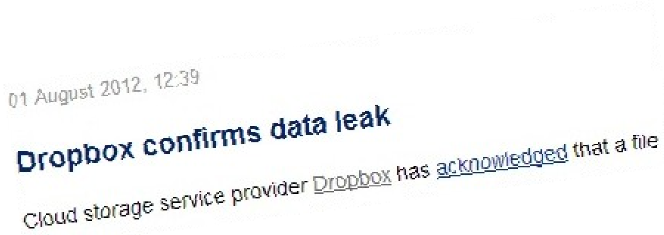
I recently received a report that attachments sent to Gmail from some servers


« Security Recommendat... | Main | Solaris Security

Amazon S3 Silent Data Corruption

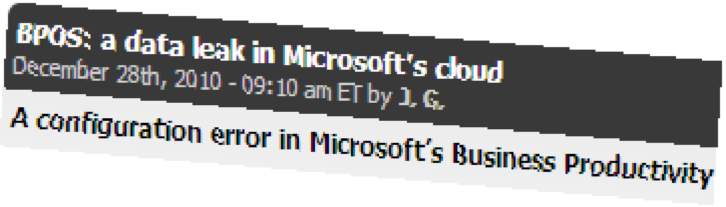
By user12606733 on Jan 28, 2009

While catching up on my reading, I came across an interesting article focused on tl


01 August 2012, 12:39

Dropbox confirms data leak

Cloud storage service provider Dropbox has acknowledged that a file


BPOS: a data leak in Microsoft's cloud

December 28th, 2010 - 09:10 am ET by J. G.

A configuration error in Microsoft's Business Productivity

ILOVEYOU worm

- Computer worm that affected million of users on May 5th 2000
- It was an email that contained a “text file” as an attachment
- Opening the attachment would activate a script, which would overwrite image files, and would send a copy of itself to the first 50 addresses in the address book
- http://en.wikipedia.org/wiki/ILOVEYOU
- **Problem**: Human factor

T-Mobile data loss

- In 2009, T-Mobile and Danger, the Microsoft-owned subsidiary that makes the Sidekick, announced that they lost all user data that was being stored on Microsoft’s servers due to a server failure
- http://techcrunch.com/2009/10/10/t-mobile-sidekick-disaster-microsofts-servers-crashed-and-they-dont-have-a-backup/
- **Problem**: Not sufficient back-ups

Factoring RSA keys

- Researchers recently showed that a bunch of cryptographic keys used in hardware devices are insecure
- Companies shipped new updates after notified
- https://factorable.net/
- **Problem**: Same randomness used across devices to generate the keys

Heartbleed

- April 2014
- Bug in the openssl library
- Affected all hosts running TLS protocol
- At the time of the disclosure, around half a million of the Internet's secure web servers certified were believed to be vulnerable to the attack
- Bug in the heartbeat feature http://tools.ietf.org/pdf/rfc6520.pdf
- There was no bound check in the bytearray that the sender would send to the receiver
- So the receiver would send the payload back along with some contents of its memory

LinkedIn passwords leaked

- In June 2012, it was announced that almost 6.5 million LinkedIn passwords were leaked and posted on a hacker site
- http://www.huffingtonpost.com/2012/06/07/linkedin-password-hack-check_n_1577184.html
- **Problem**: Linkedin did not use salt when hashing the passwords!
  - http://www.stormpath.com/blog/how-linkedin-could-have-secured-hacked-passwords