


PURDUE UNIVERSITY

Computer Security CS 426 Lecture 1

Overview of the Course



Elisa Bertino
Purdue University
IN, USA
bertino@cs.purdue.edu

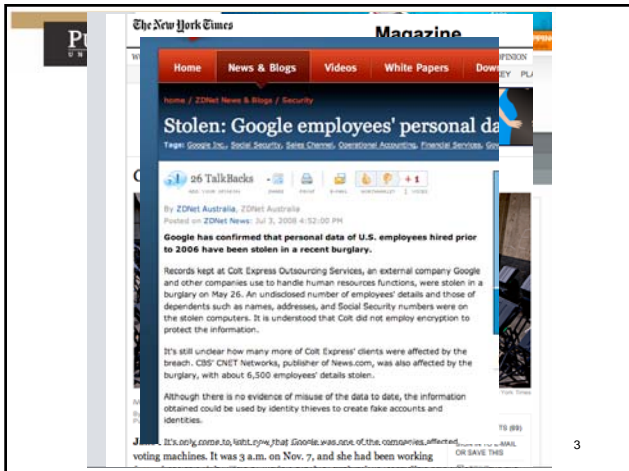
Center for Education and Research in Information Assurance and Security

PURDUE UNIVERSITY

Course Homepage

<http://www.cs.purdue.edu/homes/bertino/426Fall2009/426fall.htm>

2



The New York Times Magazine

Home News & Blogs Videos White Papers

Home / ZDNet News & Blogs / Security

Stolen: Google employees' personal data

Team: Google Inc., Social Security, Sales, Clients, Operational Accounts, Financial Services, Google

26 Talkbacks

By ZDNet Australia, ZDNet Australia
Posted on ZDNet News: Jul 3, 2009 4:52:00 PM

Google has confirmed that personal data of U.S. employees hired prior to 2006 have been stolen in a recent burglary.

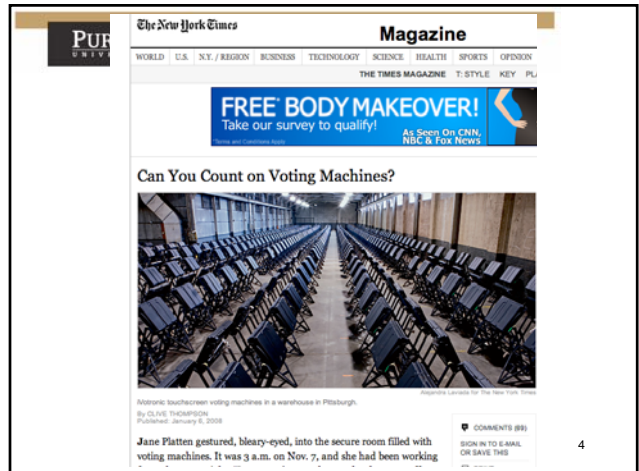
Records kept at Colt Express Outsourcing Services, an external company Google and other companies use to handle human resources functions, were stolen in a burglary on May 26. An undisclosed number of employees' details and those of dependents such as names, addresses, and Social Security numbers were on the stolen computers. It is understood that Colt did not employ encryption to protect the information.

It's still unclear how many more of Colt Express' clients were affected by the breach. CNET Networks, publisher of News.com, was also affected by the burglary, with about 6,500 employees' details stolen.

Although there is no evidence of misuse of the data to date, the information obtained could be used by identity thieves to create fake accounts and identities.

It's only come to light now that Google was one of the companies affected by the burglary. It was 3 a.m. on Nov. 7, and she had been working

3




The New York Times Magazine

WORLD U.S. NY / REGION BUSINESS TECHNOLOGY SCIENCE HEALTH SPORTS OPINION

THE TIMES MAGAZINE T: STYLE KEY PL

FREE BODY MAKEOVER!
Take our survey to qualify!
As Seen On CNN, NBC & FOX NEWS

Can You Count on Voting Machines?



Electronic touchscreen voting machines in a warehouse in Pittsburgh.

By CLIVE THOMPSON
Published: January 6, 2009

Jane Platten gestured, beary-eyed, into the secure room filled with voting machines. It was 3 a.m. on Nov. 7, and she had been working

COMMENTS (89)
SIGN IN TO EMAIL OR SAVE THIS

4

AERO YOUR DYNAMICS \$100 **FREE SHIPPING**

INTERNATIONAL Herald Tribune Europe
THE GLOBAL EDITION OF THE NEW YORK TIMES

ht.com Business Culture Sports Opinion
AMERICAS EUROPE ASIA/PACIFIC AFRICA/MIDDLE EAST TECH/MEDIA STYLE HEALTH
TRAVEL PROPERTIES BLOGS DISCUSSIONS SPECIAL REPORTS AUDIO/VIDEO

Web becomes a battleground in Russia-Georgia conflict

By John Markoff Published: August 12, 2008

SAN FRANCISCO Weeks before physical bombs started falling on Georgia, a security researcher in suburban Massachusetts was watching an attack against the country in cyberspace.

Jose Nazario of Ador Networks in Lexington noticed there was a stream of data directed at Georgian government sites containing the message win+love+in+Russia.

Other internet experts in the United States said the attacks against Georgia's internet infrastructure began as early as July 20, with coordinated barrages of millions of requests - known as distributed denial of service, or D.D.O.S., attacks - that overpowered certain Georgian servers.

Researchers at Shadowserver, a volunteer group that tracks malicious network activity, reported that the Web site of the Georgian president, Mikheil Saakashvili, had been rendered inoperable for 24 hours by multiple D.D.O.S. attacks. The researchers said the command-and-

5

PURDUE UNIVERSITY

Cyber Attacks Against SCADA and Control Systems - Real World Trends and Real World Solutions

Featuring: Eric Byres and Alan Paller

Sponsored by: **symantec.**

You need to register with the SANS portal to be able to sign in.

Webcast Overview:

Cyber Attacks Against SCADA and Control Systems - Real World Trends and Real World Solutions

Featuring: Eric Byres, Alan Paller, Bryan Giovanni Geraldo

Over the past few years the popular press has been filled with stories of terrorists using the net to attack SCADA and control systems and bring our nation to its knees. Yet the lights keep burning and the factories keep running - is the need to secure SCADA systems a myth?

Based on a careful statistical analysis of validated control system incidents at 22 major corporations, the answer is that the need to secure SCADA and Control Systems is no myth. In fact, the incidents are far more widespread than commonly believed, the targets more wide ranging and attackers are not who we think they are. Even more ominous, the data shows that getting into most control systems is surprisingly easy. The good news is data also shows that there are effective solutions for SCADA systems security. The webcast will close with a discussion of these practical and cost effective measures, particularly with respect to policy creation and management for new industry regulations like NERC CP -002-009.

Username (email):

Password:

share my info with sponsor

[Click here to proceed!](#)

[FAQ For Trouble Shooting](#)

6

PURDUE UNIVERSITY

Well Known Security and Privacy Problems

- Computer worms
 - E.g., Morris worm (1988), Melissa worm (1999)
- Computer viruses
- Distributed denial of service attacks
- Email spams
 - E.g., Nigerian scam, stock recommendations
- Identity theft
- Botnets
- Spyware

7

PURDUE UNIVERSITY

Causes of Software Security Incidents

- **Buggy software and wrong configurations...**
 - Unsafe program languages
 - Complex programs
 - Security considered rather an add-on
- **Lack of awareness and education**
 - Few courses in computer security
 - Programming text books do not emphasize security
- **Poor usability**
 - Security sometimes makes things harder to use
- **Economic factors**
 - Consumers do not care about security
 - Security is difficult, expensive and takes time
 - Few security audits
- **Human nature**

8

Human Factor

- Who are the attackers?
 - bored teenagers, criminals, organized crime, organizations, rogue states, industrial, espionage, angry employees, ...
- Why do they attack systems?
 - enjoyment, curiosity, fame, profit
 - data represents an extremely valuable asset and often the main goal of attackers is to get valuable or sensitive data

Year	Total vulnerabilities cataloged
Q1-Q3, 2008	6,058
2007	7,236
2006	8,064
2005	5,990
2004	3,780
2003	3,784
2002	4,129
2001	2,437
2000	1,090
1999	417
1998	262
1997	311
1996	345
1995	171
Totals	44,074

Goals of this Course

- Learn of to protect data and databases
- Learn to understand and apply security principles
- Learn how to prevent attacks and/or limit their consequences.
 - No silver bullet; man-made complex systems will have errors; errors may be exploited
 - Large number of ways to attack
 - Large collection of specific methods for specific purposes
- Learn to think about security when doing things

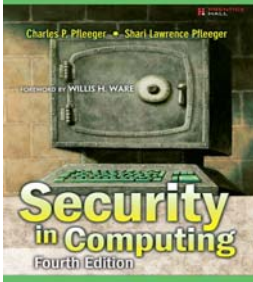
Course Outline

- Security principles
- Review of cryptography
- Operating systems security
- Database security and privacy
- Elements of network security
- Legal and ethical issues

PURDUE UNIVERSITY

Reference Material

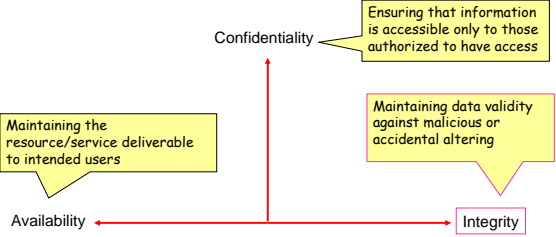
- Textbook
 - Security in Computing, C. Pfleeger and S. L. Pfleeger
- Additional papers will be assigned in class



13

PURDUE UNIVERSITY

Basic security-related requirements: the CIA triad



Confidentiality: Ensuring that information is accessible only to those authorized to have access

Availability: Maintaining the resource/service deliverable to intended users

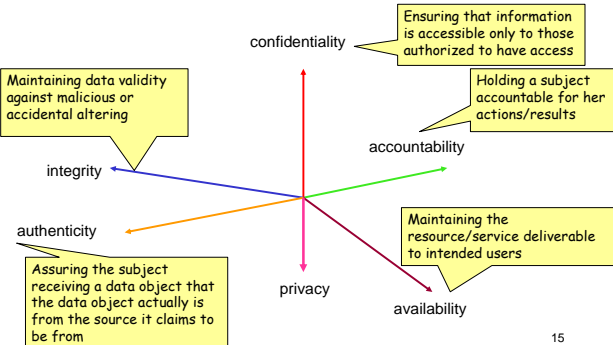
Integrity: Maintaining data validity against malicious or accidental altering

Note: Integrity is a broader notion preserving integrity of an item means that the item is: precise, accurate, consistent, meaningful and useful modified only: in acceptable ways, by authorized people, by authorized processes

14

PURDUE UNIVERSITY

Other requirements



confidentiality: Ensuring that information is accessible only to those authorized to have access

integrity: Maintaining data validity against malicious or accidental altering

authenticity: Assuring the subject receiving a data object that the data object actually is from the source it claims to be from

accountability: Holding a subject accountable for her actions/results

privacy: Maintaining the resource/service deliverable to intended users

availability: Maintaining the resource/service deliverable to intended users

15

PURDUE UNIVERSITY

Other Requirements

- Accountability: Holding a subject accountable for her actions/results
- A particular case of accountability is non-repudiation, where responsibility for an action cannot be denied
- NIST defines non repudiation as:
 - Assurance that the sender of information is provided with **proof of delivery** and the recipient is provided with **proof of the sender's identity**, so neither can later deny having processed the information.

16

Other Requirements

- Privacy: maintaining confidentiality of personally identifiable information
- (1) The ability of an individual or organization to control the collection, storage, sharing, and dissemination of personal and organizational information.
- Note: The concept of privacy cannot be very precise, because privacy relates to 'rights' that depend on legislation.

17

Terminology

- Vulnerabilities (weaknesses)
- Threats (potential scenarios of attack)
- Attacks
- Controls (security measures)

18

Methods of Defense

- Prevention
- Deterrence
- Deflection
- Detection
- Recovery

19

Controls

- Encryption
- Software controls
- Hardware controls
- Policies and procedures
- Physical controls

20

Layers of Computer Systems

- Computer systems have multiple layers
 - Hardware
 - Operating systems
 - Database systems
 - Applications
- Computer systems are connected through networks
- Computer systems are used by humans

21

Readings for this Lecture

Security in Computing
Chapter 1: Introduction

22

Acknowledgments

The course slides are partially based on slides by:

Prof. Ninghui Li

Prof. Lorenzo D. Martino

Prof. Cristina Nita-Rotaru

23