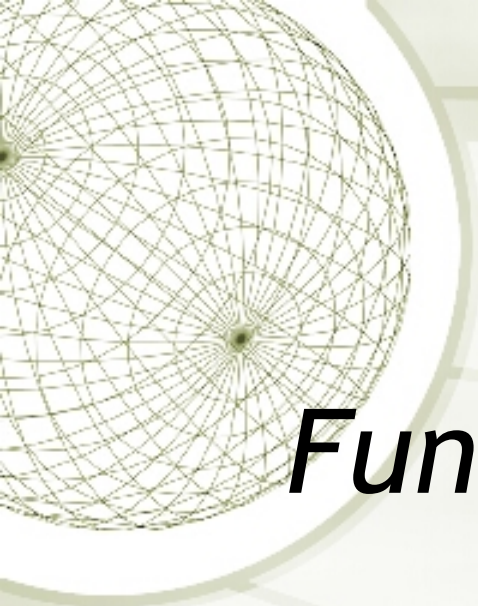
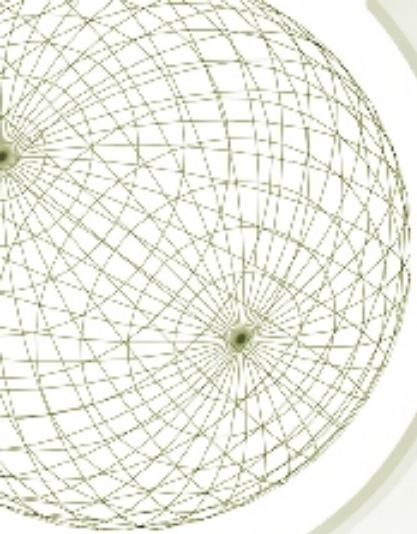


Fundamental Concepts of Data Security

Introduction

Unit Objectives

- Key concepts and approaches that are fundamental to data security
- Detailed coverage of major aspects of data security
  - security goals and general approaches to protecting data and information
  - security controls (administrative, physical, technical)
  - business continuity
  - ethics




backup
breach
masking
defense
technical
phishing
preventive
password
ethics
education
confidentiality
system
security
controls
Biba
spoofing
firewalls
disaster
TCB
erasure
deterrent
business-continuity
erasure
trusted
laws
integrity
data
Bell-Lapadula
intrusion
domain
countermeasure
countermeasure
minimization
administrative
subject
trust
quantitative
denial-of-service
threat
policy
incidents
availability
risk
Clark-Wilson
social-engineering
detection
vulnerability
recovery
qualitative
physical
computing
malicious
social
object

Introduction

- Topics to explore
  - what is security and how it has changed over time
  - what is needed to have an effective security system
  - what are the principles of security
  - what are the broad guidelines in terms of past security standards
- Security policy and procedures
  - information classification
  - education
  - risk analysis

What is data security?

- Data: information
- Data security
  - Practice of protecting information
  - Mitigate risks
  - Balanced approach: confidentiality, integrity, availability

Information Systems

- Six components
  - Data: database records, files, documents…
  - Software: applications, operating systems…
  - Hardware: server, UPS, usb devices…
  - Network: cables, routers, LANs, WiFi…
  - People/Users: administrators, normal users…
  - Procedures: security policies, continuity plans, incident response plans…

Historical Perspective

- Security used to be much different
  - Systems used to be tightly controlled and were centralised
  - Access to the system was limited
  - Access to information was easier to check and review
- Modern security is much more challenging
  - information is often sent via unsecured channels
  - computing equipment is more diverse and thus integration is always a key security issue
  - more threats to be addressed when being online

Why Data Security?

Former AWS software engineer arrested over massive Capital One data leak - Security

The United States Federal Bureau of Investigation has arrested a former Amazon Web Services Engineer, Paige Adele Thompson, for exfiltrating large amounts of data on customers of the Capital One bank.

Thompson is alleged to have accessed about 100 million credit card applications as well as US social security numbers, stored on Capital One's AWS Simple Storage Service (S3) facility.

In the court documents [pdf], the authorities allege the 33-year-old Thompson used web application firewall commands between March 12 and July 17 this year to obtain credentials for an S3 administrator role.

With the admin credentials in hand, Thompson is alleged to have viewed the data in Capital One's S3 buckets, and also exfiltrated large amounts of information via a Swedish virtual private network provider, IPredator.

While Thompson used a VPN and The Onion Router (TOR) exit nodes to hide her activities on S3, she posted files related to the illegal data access on open source code repositories Github and Gitlab using accounts bearing her full name according to FBI investigators.

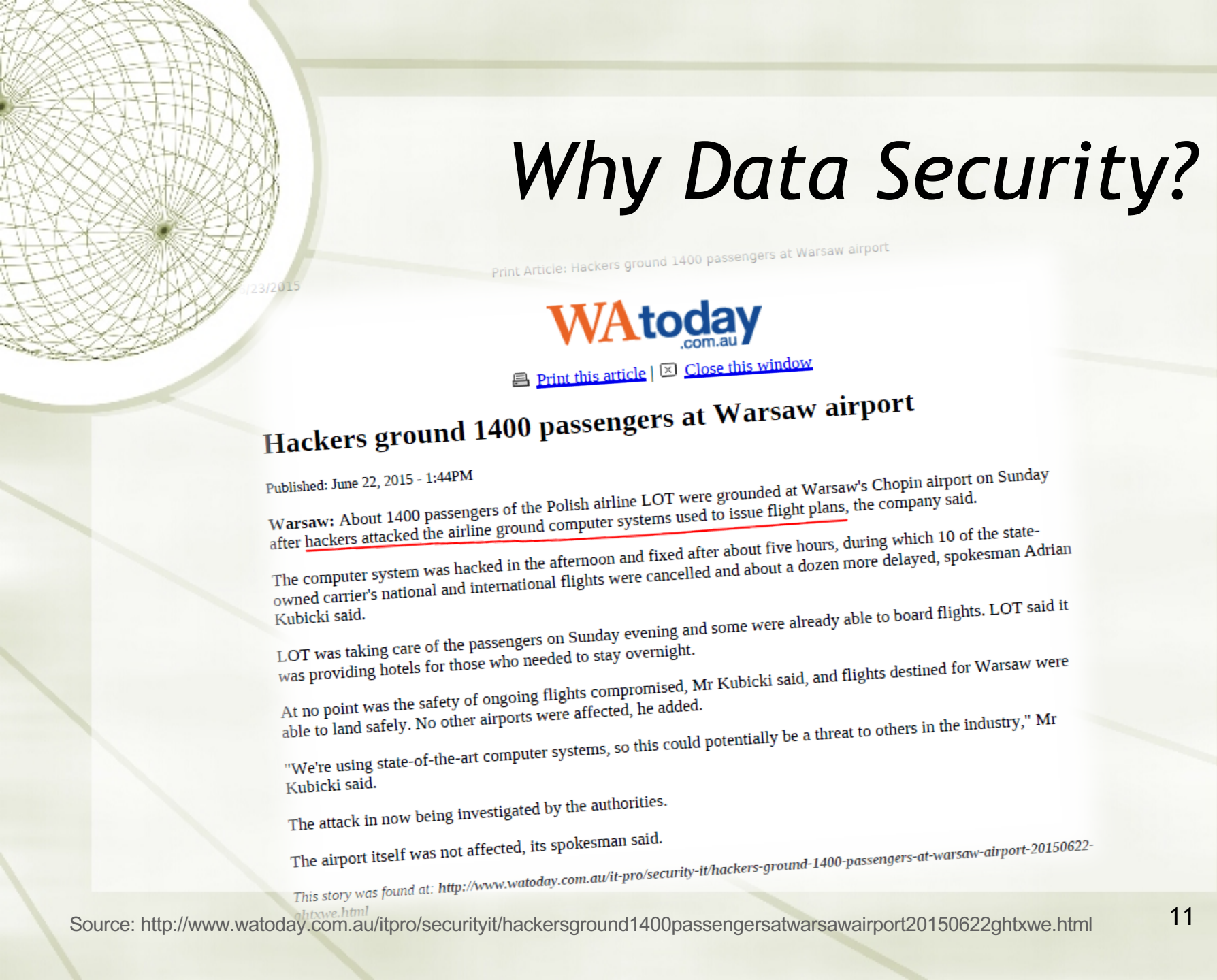
Source: https://www.itnews.com.au/news/former-aws-software-engineer-arrested-over-massive-capital-one-data-leak-528853

Why Data Security?

Fig. 2: Most Noticeable Data Exfiltration incidents in 2017

F. Ullah, R. Ramdhany, M. Edwards, and R. Chitchyan. Data Exfiltration: A Review of External Attack Vectors and Countermeasures. Journal of Network and Computer Applications · November 2017

Why Data Security?



Print Article: Hackers ground 1400 passengers at Warsaw airport

WAtoday.com.au

Print this article | Close this window

Hackers ground 1400 passengers at Warsaw airport

Published: June 22, 2015 - 1:44PM

Warsaw: About 1400 passengers of the Polish airline LOT were grounded at Warsaw's Chopin airport on Sunday after hackers attacked the airline ground computer systems used to issue flight plans, the company said.

The computer system was hacked in the afternoon and fixed after about five hours, during which 10 of the state-owned carrier's national and international flights were cancelled and about a dozen more delayed, spokesman Adrian Kubicki said.

LOT was taking care of the passengers on Sunday evening and some were already able to board flights. LOT said it was providing hotels for those who needed to stay overnight.

At no point was the safety of ongoing flights compromised, Mr Kubicki said, and flights destined for Warsaw were able to land safely. No other airports were affected, he added.

"We're using state-of-the-art computer systems, so this could potentially be a threat to others in the industry," Mr Kubicki said.

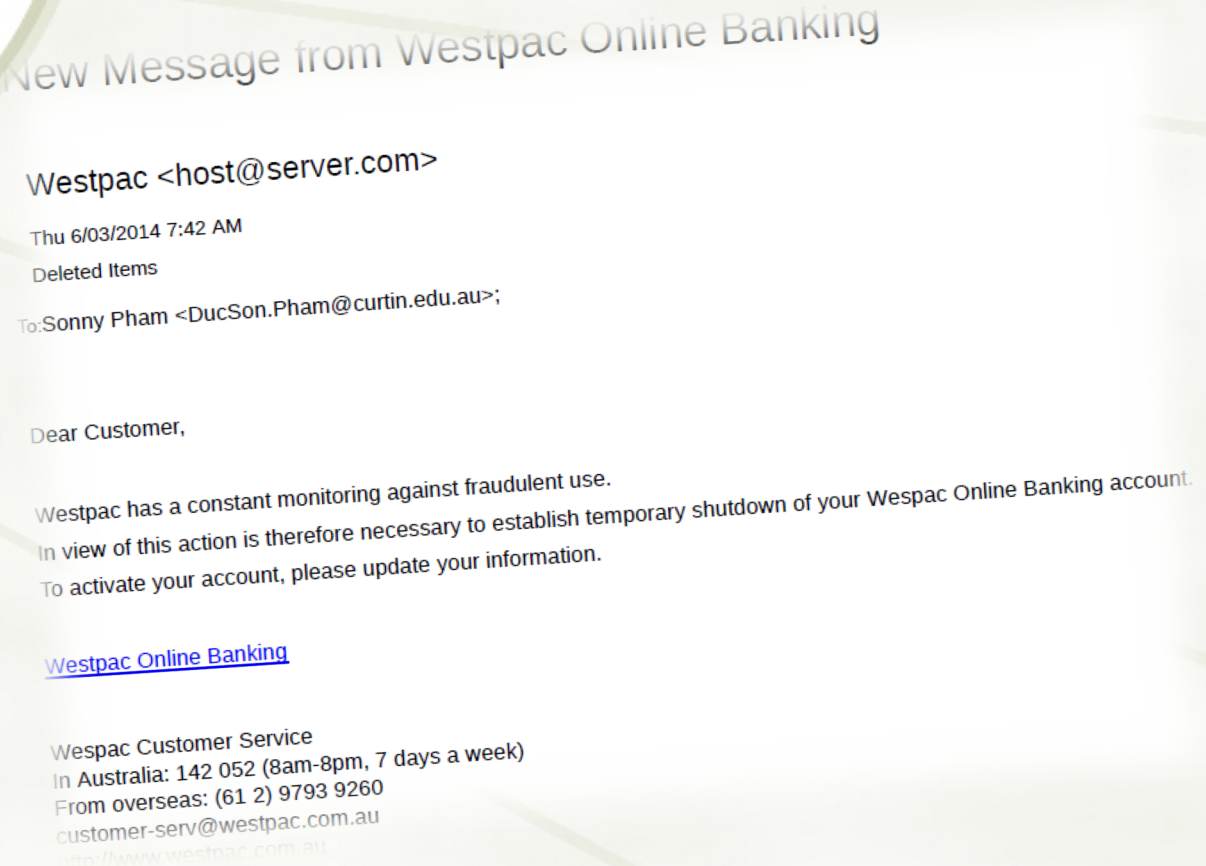
The attack in now being investigated by the authorities.

The airport itself was not affected, its spokesman said.

This story was found at: http://www.watoday.com.au/it-pro/security-it/hackers-ground-1400-passengers-at-warsaw-airport-20150622-ghtxwe.html

Source: http://www.watoday.com.au/itpro/securityit/hackersground1400passengersatwarsawairport20150622ghtxwe.html

Why Data Security?



New Message from Westpac Online Banking

Westpac <host@server.com>

Thu 6/03/2014 7:42 AM

Deleted Items

To:Sonny Pham <DucSon.Pham@curtin.edu.au>;

Dear Customer,

Westpac has a constant monitoring against fraudulent use.
In view of this action is therefore necessary to establish temporary shutdown of your Wespac Online Banking account.
To activate your account, please update your information.

Westpac Online Banking

Wespac Customer Service
In Australia: 142 052 (8am-8pm, 7 days a week)
From overseas: (61 2) 9793 9260
customer-serv@westpac.com.au
http://www.westpac.com.au

Why Data Security?

Hot issues

Fraudulent mobile number porting and identity theft

Recently ACCAN has heard increasing reports about fraudulent mobile number porting and identity theft.

What is a mobile number porting scam?

Fraudulent mobile number porting happens when a scammer uses your personal details to port your mobile number from one provider to another. Scammers can get access to your personal details, such as your date of birth, phone number and address, via your social media profiles.

Scammers then use your mobile number to gain access to email accounts and bank account details. Once your number has been ported, you no longer have access to it which means that any verification codes being sent to you by your bank for large money transfers will be sent to a scammer instead. This means they can authorise these transfers and steal money from you.

Source: [illegible]issues/1385-fraudulent-mobile-number-porting-and-identity-theft

Why Data Security?

Source:https://www.abc.net.au/news/2019-07-08/microsoft-windows-vulnerability-bluekeep-and-cyber-security-risk/11277270

Why Data Security?

Weak passwords in WA Government agencies are putting sensitive data at risk

By Jacob Kagi

Posted Wed 22 Aug 2018, 6:19am

Cyber security breach on WA Parliament knocks out communications

By Jacob Kagi

Updated Wed 17 Feb 2016, 1:55pm

Parliament has resumed sitti... the building's ... communications.

Lenovo website hacked and defaced by Lizard Squad in Superfish protest

The hacking collective took over the Lenovo site for several hours on Wednesday, redirecting users to a slideshow of bored teenagers

Alex Hern

Thu 26 Feb 2015 21.53 AEDT

Lenovo, the PC maker at the...

Flaw in Multiple Airline Systems Exposes Passenger Data | Threatpost

Author: Lindsey O'Donnell

Up to eight airlines do not encrypt e-ticketing booking sy... open for the taking.

Researchers have discovered that multiple airline e-ticke... The security faux pas could allow bad actors on the same ... some cases even change – their flight booking details or ...

Security researchers at Wandera said that eight airlines ... check-in links through their e-ticketing systems: Southw... (low-cost airline in Australia), Thomas Cook Transavia ...

Outage

Subscribe

Update - We are in-process of restoring impacted services and beginning to see some systems recover.

...have identified the networking issue ... working on a fix.

...a datacenter networking outage.

Syllabus

- This unit will cover the key aspects of data security from the point of view the three underpinning security principles: **Confidentiality, Integrity and Availability**.
- The content will cover the extension of the fundamental model **CIA** and will introduce the key concepts of risk management in an information security context.
- Data security can be provided through a range of **controls** and technologies which will be covered in detail. This will include administrative, physical and logical controls as well the processes required to handle incidents, change management and **business continuity** (and disaster planning and recovery).
- Finally, the unit will cover data backups, data masking/encryption and data erasure that is compliant with international standards.