Birkbeck
UNIVERSITY OF LONDON

Information Security & Information & Network Security Lecture 1

David Weston

Birkbeck, University of London

Autumn Term 2017

Lectures, Labs, Assessment

- Each Monday evening 18:00-21:00
- Two laboratory sessions (week 4 & week 8)
- This module will be assessed 80% by written exam in May/June and 20% from pieces of coursework that will be set during this term (the first one will be set in Week 4).
- 2 Revision Lectures in the Summer Term

Accessing module resources

- You can access copies of the lecture notes, lab sheets, class work, class work solutions etc. from the Bloomsbury Learning Environment (BLE), at

  `http://moodle.bbk.ac.uk/`

- For the next couple of weeks, the material may be found on my website:
  `http://www.dcs.bbk.ac.uk/~dweston/`

Differences

- Information Security
  - Week 7 - Reading week (Information Security at home)
  - 2 items of coursework. Week 4 and Week 9.
  - Two weeks to complete each coursework.
- Information & Network Security
  - Week 7 - Examples of Cryptographic Protocols. Chip & PIN
  - Coursework, same as Information Security, i.e. Week 4, Week 9. Two weeks to submit
  - Postgraduates students have one further coursework released in Week 7. Have until beginning of next term to submit.

Books

Main texts - Recommended

- Keith M. Martin, Everyday Cryptography: Fundamental Principles and Applications, 2012, ISBN 978-0-19-969559-1
- Ross Anderson, Security Engineering 2nd edition, John Wiley & Sons, 2008, ISBN 978-0-470-06852-6
  Available online at
  `http://www.cl.cam.ac.uk/~rja14/book.html`

We use some material from:

- William Stallings, Cryptography and Network Security 5th edition, Pearson, 2010, ISBN 978-0136097044
- Matt Bishop, Computer Security: Art and Science, Addison-Wesley, 2002, ISBN 978-0201440997
- Bruce Schneier, Applied Cryptography, John Wiley & Sons, 1996, ISBN 0-471-11709-9

Motivation

Introduction

- Protecting information against malicious or accidental access plays an important role in information-based economies/societies
- Just to name a few application areas:
  - Banking: online banking, PIN protocols, digital cash
  - Economy: mobile phones, DVD players, Pay-per-View TV, computer games
  - Military: IFF (Identification, friend or foe), secure communication channels, weapon system codes
- It's surprising how much still goes wrong in these areas

Typical Cases of Security Lapses

- Loss of confidential data:
  - 2007: HMRC loses (unencrypted) disks containing personal details of 25 million people
  - 2008: HSBC loses disks containing details of 180,000 policy holders (fined for a total of £3.2 million)
  - 2007: hard disk containing records of 3 million candidates for driver's licenses goes missing
  - not just happening in the UK: Sunrise (Swiss ISP) exposes account names and passwords of users in 2000

Typical Cases of Security Lapses (2)

- Credit card fraud is a recurring theme, ranges from
  - spying out PINs at ATMs to
  - organized stealing and trading of credit card numbers
- One example of a high profile case:
  - In the U.S. Albert Gonzalez and other hackers infiltrated Heartland and Hannaford (two firms processing payments)
  - They stole millions of credit card numbers between 2006 and 2008
  - This has cost Heartland at least $12.5 million much of which in fines

Typical Cases of Security Lapses (3)

- Hacking into other systems:
  - 2008: in the U.S. 18-year old student hacks into high school computer, changes grades
  - 2005: UCSB (University of California Santa Barbara) student hacks into eGrades system and changes grades
  - 2012: LinkedIn, hashed passwords leaked. Passwords not salted.
  - 2014: Heatmiser - digital thermostat that has multiple security lapses including default username/password
  - See for example: `http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/`

Typical Cases of Security Lapses (4)

- Denial-of-Service attacks:
  - 2009: Twitter is hit by a denial-of-service attack and brought to a standstill
- Natural disasters (cause needs not be malicious):
  - Data loss through fire, storm, flooding
  - Accounts for approximately 3% of all data loss

Objective

- This list could go on and on . . .
- However, even this small number of examples already shows the importance of this subject
- Objective of this module is to teach basic principles of information security, enabling you to
  - identify and assess security risks
  - take appropriate countermeasures

Introduction

Basic Definitions

- How do we define *information security*?
- Information security is about ensuring the following:
  - Confidentiality
  - Integrity
  - Availability

Confidentiality

- *Confidentiality* is (the principle of) restricting access to information
- Only people who are authorized should be able to access information
- Example for loss of confidentiality: losing disks with sensitive data

Integrity

- *Integrity* is about preventing improper or unauthorized change of data
- Only trustworthy data is of value
- Example for loss of integrity: student hacking into university computer and changing grades

Availability

- *Availability* is about making sure that information is accessible when needed (by authorized persons)
- Usually this implies keeping systems that store the information (and restrict access) operational
- Example for loss of availability: system taken out by a disaster

Additional Aspects

- Sometimes the following aspects are added as separate issues:
  - Authentication: confirming the identity of an entity
  - Non-repudiation: an entity is not able to refute an earlier action

Threats, Attacks, and Vulnerabilities

- A *threat* is a potential danger to an (information) asset, i.e. a violation of security might occur
- An *attack* is an action that actually leads to a violation of security
- A *vulnerability* is a weakness that makes an attack possible

Threats, Attacks, and Vulnerabilities (2)

- An example: a server storing source code for a new product of a software development company
  - Threat: an unauthorized person (e.g. from a competitor) could access the source code
  - Attack: someone (unauthorized) actually logs into the system and downloads (parts of) the source code
  - Vulnerability: an unremoved test account with a default password

Security Controls

- Security *controls* are mechanisms to protect information (or a system) against
  - unauthorized access (ensuring confidentiality)
  - unauthorized modification (ensuring integrity)
  - destruction/denial-of-service (ensuring availability)
- Controls are also called *countermeasures* or *safeguards*
- General types of controls:
  - Physical
  - Technical
  - Administrative

Physical Controls

- Physical Controls include the following:
  - locks
  - security guards
  - badges/swipe cards/scanners
  - alarms
  - fire extinguishers
  - backup power
  - ...

Technical Controls

- Technical controls include the following:
  - access control software/passwords
  - antivirus software
  - encryption
  - backup software/systems
  - ...

Administrative Controls

- Administrative controls include the following:
  - staff training
  - clear responsibilities
  - policies and procedures
  - contingency plans
  - ...

Controls Covered in This Course

- In this course we are going to focus on
  - technical controls
  - administrative controls
- Although physical controls should be kept in mind, we don't have enough time to cover everything
- The other two controls are more interesting from the point of view of computer science and management

Controls Covered in This Course (2)

- Why not just look at the technical issues?
- Security is only as strong as the weakest link
- Very often, people are the weakest link

Overview

- In the first part of this module, we're going to cover the administrative side
- Second part looks at the technical side
- More fine-grained overview of what's to come:
  - Administrative Issues
  - Risk Assessment
  - Security Policies
  - Social Engineering
  - Cryptography
  - Cryptographic Protocols
  - Selected Topics

Administrative Issues

Organizational Environment

- No matter how small the organization, there has to be someone responsible for information security
- Usually, this person is called the *security officer* or *SO* (or some other acronym)
- In small- or medium-sized organizations could be an added responsibility (not a full portfolio)
- In large organizations, SO might be supported by a team

Role of Security Officer

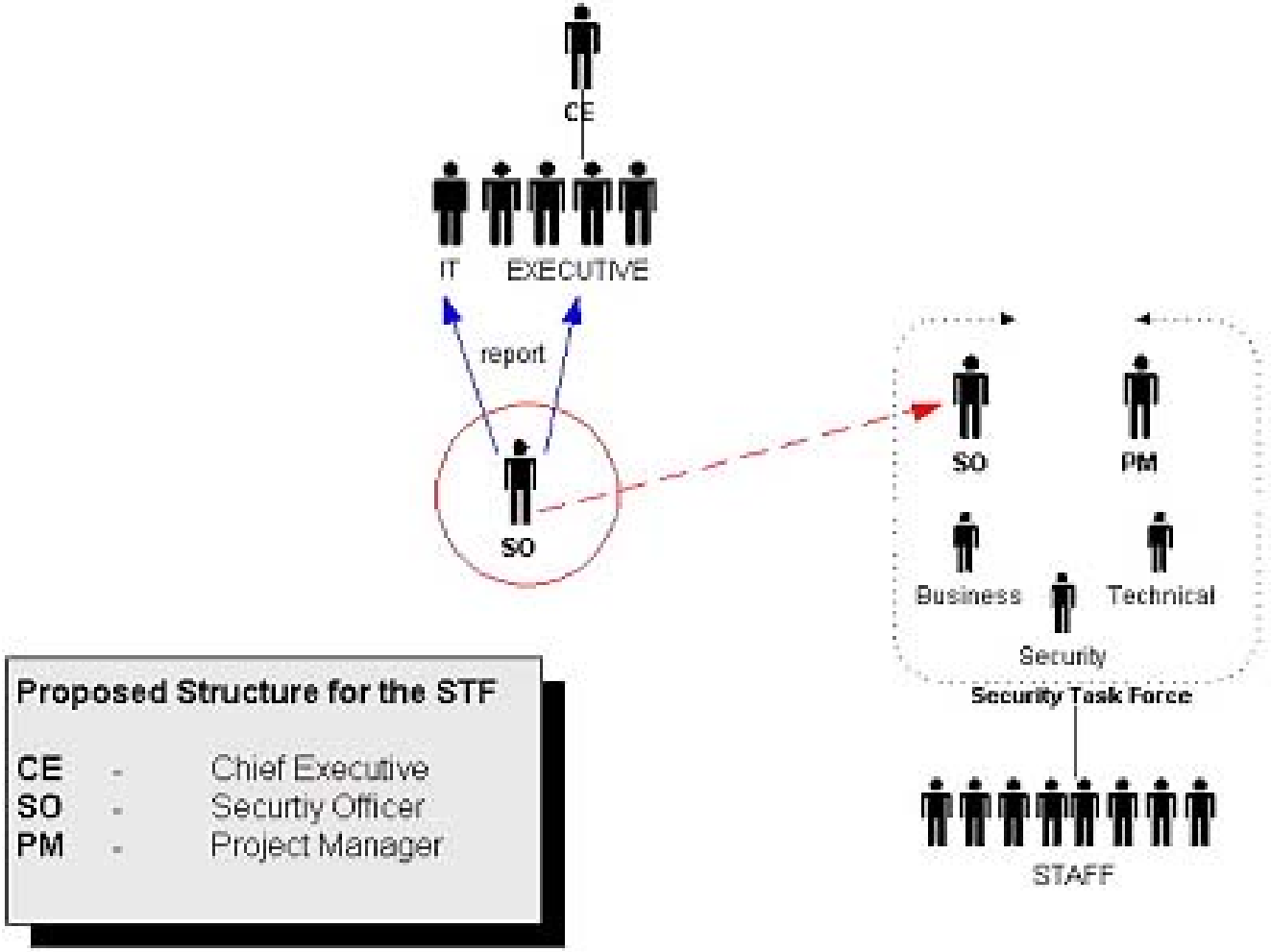
- Defines a corporate security policy
- Defines system-specific security policies
- Creates project plan for implementing controls
- Responsible for user awareness and training programs
- Appoints auditors
- Optional: obtains formal accreditation

Place in Hierarchy of SO

- Due to the importance of information security
  - SO should report to the highest level of control (board of directors, CEO)
  - SO may even be a member of the board
- SO acts as an intermediary between management and the user base

Place in Hierarchy of SO (2)

- Example for a large organization:



Management Support

- In order for SO to be successful, they need support from high-level management
- Convincing (top-level) management can be difficult
  - Ignorance of real nature of risks
  - Fixated on bottom line (security costs money, no clear benefits)
  - Fear of having to address unknown risks and take responsibility

Convincing People

- Introducing security measures will always require investments in time, human resources, and money
- Not doing so, however, can have dire consequences:
  - HSBC having to pay a fine of £3.2 million
  - Heartland losing at least $12.5 million
  - Health services and software companies in the U.S. have been sued for millions or even billions of dollars
  - Bloghoster JournalSpace had to close shop after losing all content data
- First important step: know your exposure to risk

Risk Assessment

What is It About?

- *Risk assessment* helps in understanding:
  - What is at risk? (Identifying assets)
  - How much is at risk? (Identifying values)
  - Where does the risk come from? (Identifying threats and vulnerabilities)
  - How can the risk be reduced? (Identifying countermeasures)
  - Is it cost effective? (Risk can never be completely eliminated)

Traditional Method

- Single Loss Expectancy (SLE): measures the expected impact (in monetary terms) of a certain threat occurring:

$$\text{SLE} = \text{Asset Value (AV)} \times \text{Exposure Factor (EF)}$$

- Asset Value is the total value of the asset under threat
- Exposure Factor measures the proportion of the asset that is lost when threat becomes real
  - Range is between 0.0 and 1.0
  - 1.0 meaning the complete asset is lost

Traditional Method (2)

- Usually this is looked at on an annualized basis
- Annualized Rate of Occurrence (ARO) represents the expected frequency of a threat occurring per year
- This gives us the Annualized Loss Expectancy (ALE):

$$\text{ALE} = \text{SLE} \times \text{ARO}$$

- The tricky part is figuring out all these values (more on this later)

Simple Example

- We have an asset worth £150,000, so AV = £150,000
- If threat occurs, we lose two thirds of it, so EF = 2/3
- We expect this threat to occur once every 20 years (on average), so ARO = 0.05
- This gives us:

$$\text{ALE} = £150{,}000 \times 2/3 \times 0.05 = £5000$$

Example from Banking

- An ALE analysis for a bank's computer systems might have hundreds of different entries, e.g.

Loss Type	Asset Value	ARO	ALE
SWIFT fraud	£30,000,000	0.005	£150,000
ATM fraud (large)	£200,000	0.2	£40,000
ATM fraud (small)	£15,000	0.5	£7,500
Teller takes cash	£2,160	200	£432,000

- Here we assume that EF = 1.0, i.e. all the money is lost
- Accurate figures are probably available for common losses, much harder to get these numbers for uncommon, high-risk losses

Putting Controls in Place

- Introducing controls/countermeasures has an effect on the rate of occurrence and/or the exposure factor
- So we have ALE_{before} and ALE_{after}
- We reduce risk by

$$ALE_{before} - ALE_{after}$$

- However, controls also have an annual cost: $AC_{control}$
- So, the overall benefit is

$$(ALE_{before} - ALE_{after}) - AC_{control}$$

Risk and Information Assets

- What does this all mean for risk assessment in the context of information security?
- We have to analyze different aspects:
  - Value of the information/system assets
  - Possible threats to information/systems
  - Vulnerabilities of information/systems
  - Cost of countermeasures

How to Measure Risk

- Risk is a function of threats, vulnerabilities, and assets:

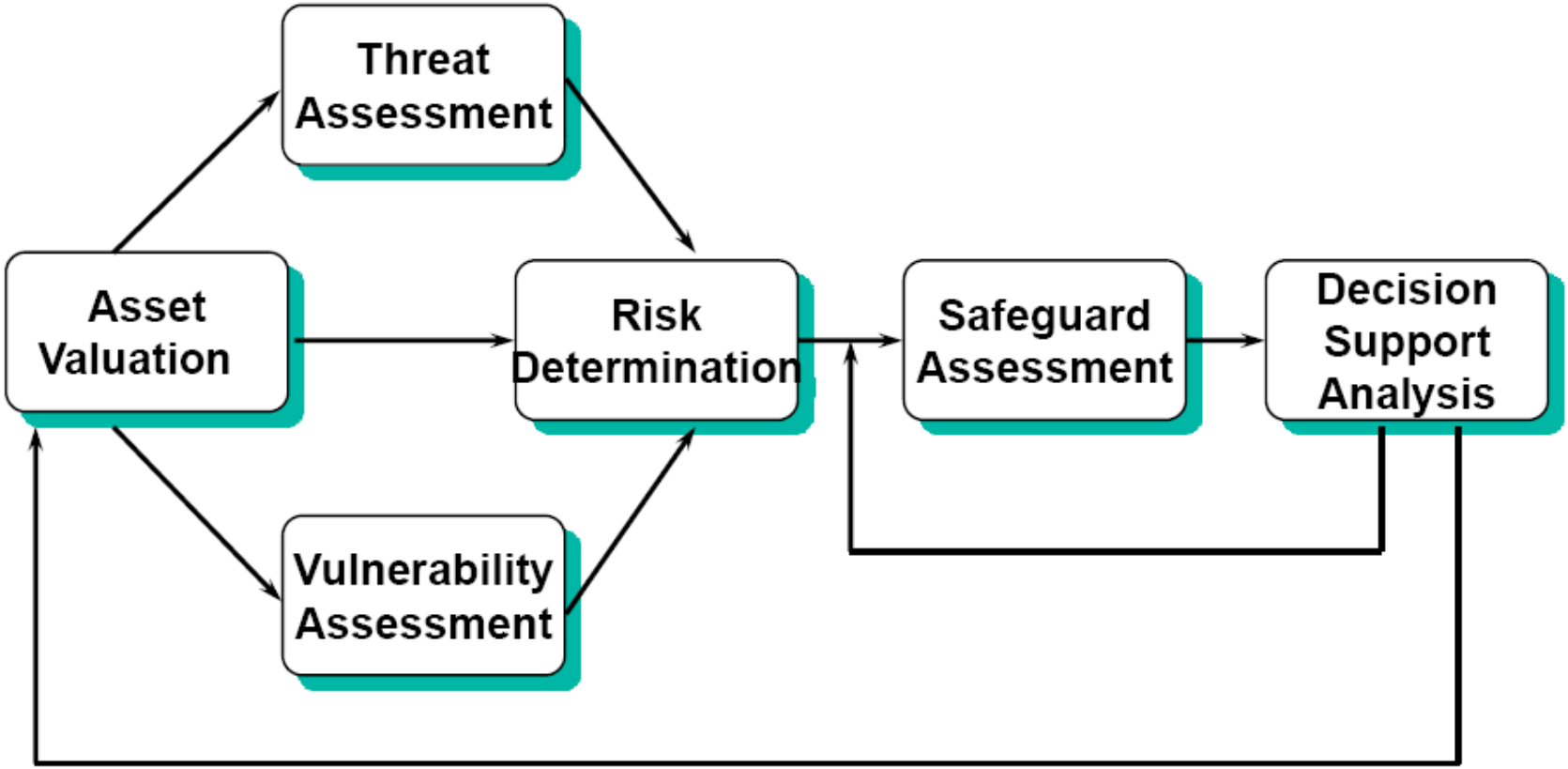
How to Measure Risk (2)

- With the help of controls, the risk can be reduced:

How to Measure Risk (3)

- Example of reducing threat:
  - Do a background check on employees
- Example of reducing vulnerability:
  - Keep system updated, i.e. install patches
- Example of reducing asset (value):
  - Encrypt data: even if it is accessed, it's worthless

Overall Assessment Process



Asset Valuation

- Basically two different kinds of assets:
  - Tangible assets (hardware, buildings, etc.)
  - Intangible assets (software, information)
- Valuing tangible assets and part of the intangible assets (operating systems and application software) is not too hard
  - They have a price tag
  - Cost to replace them is known
- What about information assets?

Information Asset Valuation

- One way to put a value on information assets is to ask knowledgeable staff
- Delphi method is used to do this in a systematic way

Delphi Method

- Experts (i.e. knowledgeable staff) give answers to questionnaires for several rounds
- After each round a facilitator summarizes answers (and reasoning) given by experts
- This summary is given to the experts (usually done anonymously)
- New round is started in which experts may revise their answers

Approach by Zareer Pavri

- Use a cost-based and/or income-generating approach to arrive at concrete numbers
- Cost approach: try to put a fair market value on the information assets
- Income approach: try to determine income stream generated by products/services associated with information assets
- However, even Zareer Pavri admits that valuation of information assets is sometimes more of an art than a science

Example for Gillette

- In 1998 Gillette had a total value of invested capital of $58.53 billion
  - This is based on a market price of $49 per share
  - Working Capital was $2.850 billion
  - Fixed/other assets were at $5.131 billion
  - Intangible assets (with a price tag) $5.854 billion
- We are missing $44.7 billion
- At least part of this has to be the value of the information assets

Threat Analysis

- Let's move to the next point: threat analysis
- Reminder: a threat is a potential danger to an asset
- Generally there are two different types:
  - Accidental
  - Intentional
- Many different sources are possible:
  - Natural: floods, fires, earthquakes, ...
  - Human: network-based attacks, malicious software upload, incorrect data entry, ...
  - Environmental: power failure, leakage, ...

Threat Analysis (2)

- During threat analysis, analyst must decide which threats to consider
- This can be a formidable task:
  - There's always the danger of overlooking something
  - It's impossible to protect yourself against every possible threat
- Fortunately, many other people have done this before
  - An analyst does not have to start from scratch

Threat Analysis (3)

- Lots of different sources are available:
  - Government: CESG (Communications-Electronics Security Group), a branch within the GCHQ (Government Communications Headquarters) `www.cesg.gov.uk`
  - Industry: vendors of risk assessment tools, we'll look at one in a moment: CRAMM `www.cramm.com`
  - Hire consultants: e.g. CMU's Computer Emergency Response Team (CERT) `www.cert.org`
  - Other organizations: SANS (Sysadmin, Audit, Network, Security) Institute `www.sans.org`
  - There's also a newsgroup called comp.risks

Vulnerability Analysis

- Next task is about identifying vulnerabilities that can be exploited
- Vulnerabilities allow threats to occur (more often) or have a greater impact
- Some argue that vulnerability analysis should be done before threat analysis
  - If there is no vulnerability, there is no threat
  - However, it's not possible to eliminate each and every vulnerability

Vulnerability Analysis (2)

- Starting a vulnerability analysis from scratch would also be very tedious
- Fortunately, this has also been done before
  - The sources mentioned before also have material on vulnerability analysis
- One more source should be mentioned here:
  - National Vulnerability Database (NVD) provided by the National Institute of Standards & Technology (NIST):
    `https://nvd.nist.gov/`
  - Just for the month of September 2017, there were 1233 vulnerabilities documented in the database.

NVD Example

National Vulnerability Database (NVD)National Vulnerability Database (CVE-2007-3896) - Mozilla Firefox <2>

File Edit View History Bookmarks Tools Help

http://web.nvd.nist.gov/view/vuln/detail?execution=e3s1

Most Visited Smart Bookmarks openSUSE Getting Started Latest Headlines

Home | ISAP/SCAP | SCAP Validated Tools | SCAP Events | About | Contact | Vendor Comments

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

37412 CVE Vulnerabilities
142 Checklists
177 US-CERT Alerts
2335 US-CERT Vuln Notes
2517 OVAL Queries
17649 CPE Names

Last updated: Fri Jun 19 13:53:23 EDT 2009

CVE Publication rate: 14.8

Email List

NVD provides four mailing lists to the public. For information and subscription instructions please visit NVD Mailing Lists

Workload Index

National Cyber-Alert System

Vulnerability Summary for CVE-2007-3896

Original release date: 10/11/2007

Last revised: 09/05/2008

Source: US-CERT/NIST

Static Link: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3896

Overview

The URL handling in Shell32.dll in the Windows shell in Microsoft Windows XP and Server 2003, with Internet Explorer 7 installed, allows remote attackers to execute arbitrary programs via invalid "%" sequences in a mailto: or other URI handler, as demonstrated using mIRC, Outlook, Firefox, Adobe Reader, Skype, and other applications. NOTE: this issue might be related to other issues involving URL handlers in Windows systems, such as CVE-2007-3845. There also might be separate but closely related issues in the applications that are invoked by the handlers.

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C) (legend)

Impact Subscore: 10.0

Exploitability Subscore: 8.6

CVSS Version 2 Metrics:

Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism

Access Complexity: Medium

Authentication: Not required to exploit

Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites

Done

NVD Example (2)

National Vulnerability Database (NVD)National Vulnerability Database (CVE-2007-3928) - Mozilla Firefox <2>

File Edit View History Bookmarks Tools Help

http://web.nvd.nist.gov/view/vuln/detail?execution=e5s1

Most Visited Smart Bookmarks openSUSE Getting Started Latest Headlines

Sponsored by DHS National Cyber Security Division/US-CERT

NIST National Institute of Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities | Checklists | Product Dictionary | Impact Metrics | Data Feeds | Statistics

Home | ISAP/SCAP | SCAP Validated Tools | SCAP Events | About | Contact | Vendor Comments

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

37424 CVE Vulnerabilities
142 Checklists
177 US-CERT Alerts
2335 US-CERT Vuln Notes
2517 OVAL Queries
17649 CPE Names

Last updated: Fri Jun 19 14:08:39 EDT 2009

CVE Publication rate: 15.2

Email List

NVD provides four mailing lists to the public. For

National Cyber-Alert System

Vulnerability Summary for CVE-2007-3928

Original release date: 07/21/2007

Last revised: 09/05/2008

Source: US-CERT/NIST

Static Link: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3928

Overview

Buffer overflow in Yahoo! Messenger 8.1 allows user-assisted remote authenticated users to execute arbitrary code via a long e-mail address in an address book entry. NOTE: this might overlap CVE-2007-3638.

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 7.6 (HIGH) (AV:N/AC:H/Au:N/C:C/I:C/A:C) (legend)

Impact Subscore: 10.0

Exploitability Subscore: 4.9

CVSS Version 2 Metrics:

Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism

Access Complexity: High

Authentication: Not required to exploit

Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

Done

Putting It All Together

- To assess risks, threats have to be connected to vulnerabilities, which have to be mapped to assets:

VULNERABILITY	MAPPED THREAT(S)	AFFECTED ASSETS (At minimum)[a]
No Logical Access Control	Sabotage of Software	Software Goodwill
	Sabotage of Data/Information	Information Integrity Goodwill
	Theft of Software	Software Goodwill
	Theft of Data/Information	Information Confidentiality Goodwill
	Destruction of Software	Software Goodwill
	Destruction of Data/Information	Information Availability Goodwill
No Contingency Plan	Fire Hurricane Earthquake Flood Terrorist Attack	Facilities Hardware Media and Supplies IT Staff Budgets Software Information Availability Goodwill
	Toxic contamination[b]	IT Staff Budgets Software Information Availability Goodwill

Risk Assessment

- We've covered asset valuation and threat & vulnerability analysis, next step is actual risk assessment
- *Risk modeling* aims at giving well-informed answers to the following questions:
  - What could happen? (threats/vulnerabilities)
  - How bad would it be? (impact)
  - How often might it occur? (frequency/probability)
  - How certain are answers to the question above? (uncertainty)

Risk Modeling

- We've covered the first question (threat and vulnerability analysis)
- Second question (impact) was covered to a certain extent (by putting values on assets)
- Uncertainty could be modeled by bounded distributions:
  - "I'm 80% certain that it will cost between £170K and £200K to reconstruct the content of this file."
- Where do we get the other numbers from?
- This is not a trivial task

Risk Modeling (2)

- Results of an FBI/CSI (Computer Security Institute) survey in 2002:
  - 80% of investigated companies reported financial losses due to security breaches, only 44% could quantify losses
  - Only 30% of UK businesses had ever evaluated return-on-investment for information security spending

Risk Modeling (3)

- People assessing risks have to rely on some form of statistical data
- This data can come from
  - internal sources (if an organization keeps records)
  - employees, customers, clients
  - other organizations such as
    - NIST
    - ASIS International (an organization for security professionals): `www.asisonline.org`
    - government, e.g. law enforcement
  - tools for risk assessment
- On top of that you need statistical methods to evaluate the data

Quantitative vs. Qualitative Assessment

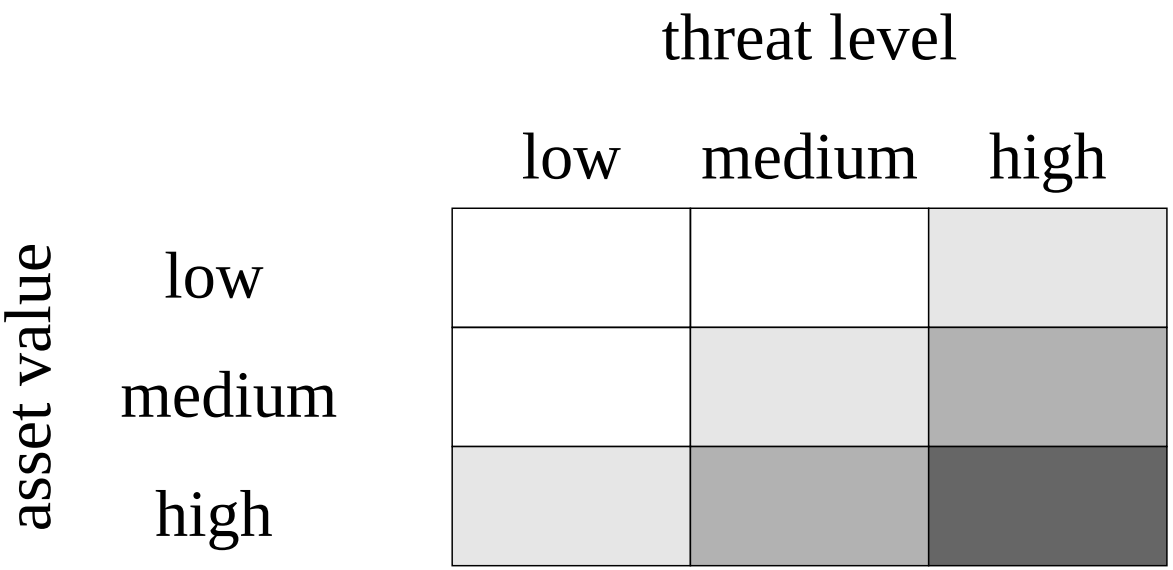
- Trying to put a number on everything is called *quantitative risk assessment*
- Computing the ALE is a classic form of quantitative risk assessment
- Prerequisites of this approach:
  - Reliable data has to be available
  - Appropriate tools are available
  - The person doing the assessment knows what they are doing (and is trustworthy)
- If this is not the case, quantitative assessment can lead to a false sense of security
  - Especially if the numbers are “massaged”

Qualitative Assessment

- An alternative to quantitative assessment is *qualitative risk assessment*
- Rather than using concrete numbers, ranking is used, e.g. describing a threat level as high, medium, or low
- Asset values may also be described in a similar way, e.g. high, medium, or low importance

Qualitative Assessment (2)

- Analysis is described with the help of a matrix:



- The darker the field, the higher the risk
- Depending on security goals, certain risk levels have to be addressed (by introducing controls)

Qualitative Assessment (3)

- Qualitative assessment is easier to understand by lay persons
- However, it has the following problems:
  - Results are essentially subjective
  - Results of cost/benefit analysis might be hard to express

Methodology

- There are pros and cons for both the quantitative and qualitative approaches
- Most important issue:
  - A knowledgeable person is doing the assessment
  - This is done in a systematic way
- The concrete methodology becomes important when you are looking for an accreditation
- Most relevant in the UK is BS 7799 (the international version of this standard is ISO 27001/27002)

Hybrid Approaches

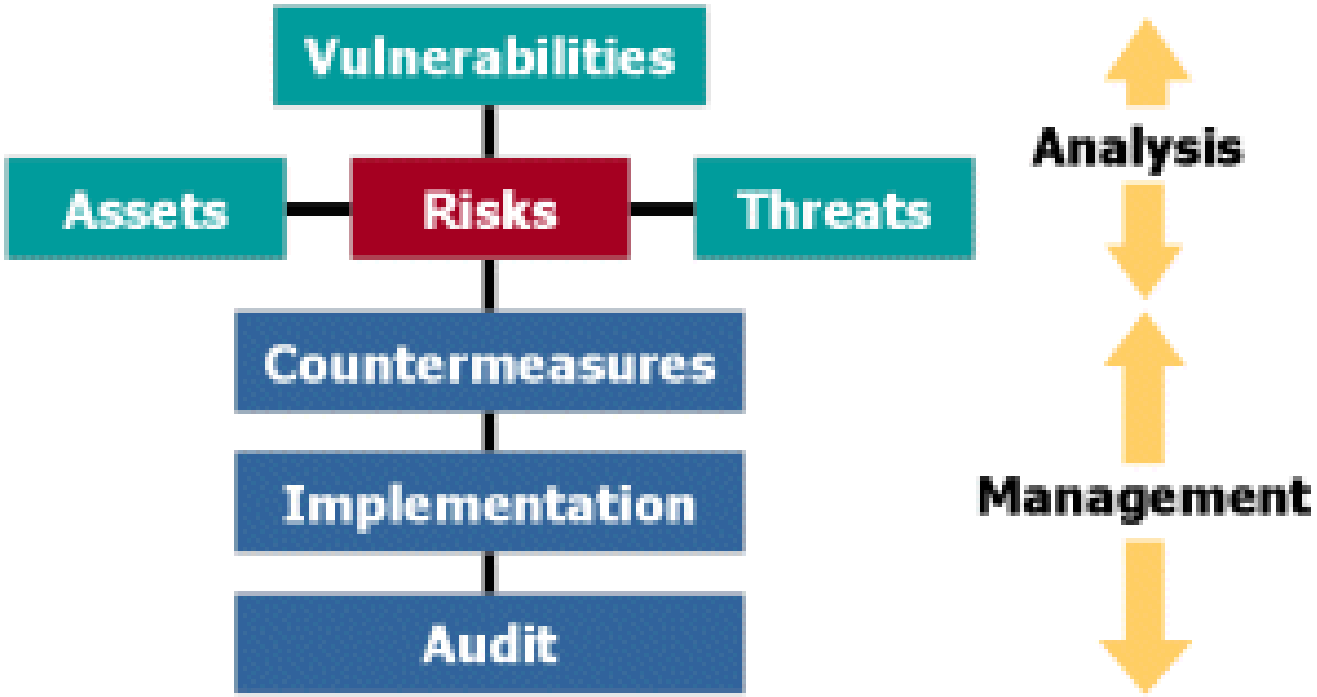
- Quantitative and qualitative risk assessment are rarely used in their pure form (in the context of information security)
- Increasing the granularity of a qualitative approach (by adding more levels) will push it into the direction of quantitative assessment
- Very often a combination of both, a *hybrid approach*, is used

CRAMM

- Let's complete the discussion on risk assessment by looking at a concrete tool: CRAMM
- CRAMM stands for CCTA Risk Analysis and Management Method
  - CCTA in turn stands for Central Computing and Telecommunications Agency
- CRAMM is ISO 27001 compliant and, e.g., used by NATO, BAE Systems Electronics, and the NHS
- If you're selling to the UK government, chances are high that you have to use this method/tool

CRAMM (2)

- CRAMM follows the following overall procedure (from top to bottom):



Screenshot: Threat/Vulnerability Analysis

Rapid Risk Assessment

Threat Type: Masquerading of User Identity by Insiders

Level for all Impacts: High

Asset Group	Impact (if specific)	Threat Level	Vuln Level	Comment
!Using Local Area Network	UNAVAIL-15ML	Very High	High	
!Using Local Area Network	UNAVAIL-1H	Very High	High	
!Using Local Area Network	UNAVAIL-3H	High	High	
!Using Local Area Network	UNAVAIL-12H	High	High	
!Using Local Area Network	UNAVAIL-1D	Medium	Low	
!Using Local Area Network	UNAVAIL-2D	Low	Low	
!Using Local Area Network	DESTR-PART	Low	High	
!Using Local Area Network	DISCL-I	Very High	High	
!Using Local Area Network	MODIF-DEL	Low	High	
!Using Stock Control System	UNAVAIL-15ML	High	High	
!Using Stock Control System	UNAVAIL-1H	Low	High	
!Using Stock Control System	UNAVAIL-3H	Low	High	
!Using Stock Control System	UNAVAIL-12H	Low	High	
!Using Stock Control System	UNAVAIL-1D	Very Low	Low	
!Using Stock Control System	UNAVAIL-2D	Very Low	Low	

Note | Status of TV Questionaires | TV Reports

How Does It Work?

- CRAMM uses a risk matrix
- However, this matrix is a bit more sophisticated than the one on a previous slide:
  - 7 levels for measuring risk: from 1 (low) to 7 (high)
  - 10 levels for asset values: from 1 (low) to 10 (high)
  - 5 threat levels: very low, low, medium, high, very high
  - 3 vulnerability levels: low, medium, high

How Does It Work? (2)

- At the core of CRAMM is the following matrix:

Threat	Very Low	Very Low	Very Low	Low	Low	Low	Medium	Medium	Medium	High	High	High	Very High	Very High	Very High
Vuln.	Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High
Asset Value															
1	1	1	1	1	1	1	1	1	2	1	2	2	2	2	3
2	1	1	2	1	2	2	2	3	3	2	3	3	3	3	4
3	1	2	2	2	2	3	2	3	3	3	3	4	3	4	4
4	2	2	3	2	3	3	3	3	4	3	4	4	4	4	5
5	2	3	3	3	3	4	3	4	4	4	4	5	4	5	5
6	3	3	4	3	4	4	4	4	5	4	5	5	5	5	6
7	3	4	4	4	4	5	4	5	5	5	5	6	5	6	6
8	4	4	5	4	5	5	5	5	6	5	6	6	6	6	7
9	4	5	5	5	5	6	5	6	6	6	6	7	7	7	7
10	5	5	6	5	6	6	6	6	6	6	7	7	7	7	7

How Does It Work? (3)

- Basically, CRAMM is a qualitative form of assessment
- However, the different levels can be roughly mapped to concrete values (making it somewhat hybrid)
- Example for mapping levels of risk to ALE:

CRAMM Measure of Risk	"Annual Loss of Expectancy"
1	<£1,000
2	<£10,000
3	<£100,000
4	<£1,000,000
5	<£10,000,000
6	<£100,000,000
7	<£1,000,000,000

Selecting Countermeasures

- Depending on the
  - type of threat
  - type of asset
  - desired security level

  a countermeasure can be selected
- CRAMM contains a library of about 3500 generic controls

Screenshot: Countermeasures

Countermeasure Tree

- System Input/Output Controls
- Network Security Management
  - Information and Software Exchange Agreements
  - Network Management
  - Network Monitoring
    - 1 The network should be monitored
      - 2 Detection and alarms for network failure
        - 3 Traffic loss detection/alarm
        - 3 Node loss detection/alarm
        - 3 Intelligent Management System
        - 3 Introduction of unauthorised devices or nodes
        - 3 Multiple address clashes
        - 3 Signal loss alarm systems
    - 1 All faults on the network should be reported
  - Security of Network Services
  - Evasion of Network Disruption

Name	Rec.	Status
Local Area Network		To be implemented

Set Status for all assets to:

Testing It Out

- After countermeasures have been put in place, everything can and should be tested in practice
- Organizations often do *penetration studies*
  - They hire a team of professional security experts who (are authorized to) try to violate the security
  - The goal is to find gaps in the implemented security

Flaw Hypothesis Methodology

- A framework for conducting these studies is:
  1. Information gathering: testers try to become as familiar with system as possible (in their role as external or internal attackers)
  2. Flaw hypothesis: drawing on knowledge from step 1 and known vulnerabilities, testers hypothesize flaws
  3. Flaw testing: tester try to exploit possible flaws identified in step 2
     - If flaw does not exist, go back to step 2
     - If flaw exists, to to next step
  4. Flaw generalization: testers try to find other similar flaws, iterate test again (starting with step 2)
  5. Flaw elimination: testers suggest ways of eliminating flaw

Example of a Study

- The Internal Revenue Service (IRS) in the U.S. did a penetration study in 2001:
  - Testers were able to identify some but not all IRS Internet gateways
  - Testers then tried to get through the firewalls of the identified gateways (but were not successful)
  - However, they gained enough information to circumvent firewalls
  - Testers, posing as Help Desk employees, called 100 IRS employees asking for assistance
  - 71 of these employees agreed to temporarily change their password to help resolve a technical problem
  - Together with a phone number (also obtained by the testers) this would have enabled them to get access

Debate on Studies

- There is an ongoing debate on the validity of penetration studies
  - Some vendors use it as an argument to prove the security of their product
  - Critics claim that these studies have no validity at all (can only show presence of flaws, not the absence)
- The answer probably lies in the middle:
  - Penetration studies are not a substitute for thoroughly designing and implementing a security solution
  - However, they are valuable in a final “testing” stage

Conclusion

- Risk assessment is an important first step in determining
  - whether to protect an asset and to which level
  - the threats to protect against and their likelihood of occurring
- Environments change, so (parts of) the assessment might have to be redone later
- Most important thing is to create an awareness and starting a risk assessment process