Security management in the Internet era

5th: Diversity of risks & countermeasures in Information Systems
October 28, 2010

Jun Murai
Keio University

Suguru Yamaguchi
Nara Institute of Science and Technology

Schedule

01st（09/30）	Course Description
02nd（10/07）	Internet becomes infrastructure (1)
03rd（10/14）	Internet becomes infrastructure (2)
04th（10/21）	Internet becomes infrastructure (3)
05th（10/28）	Diversity of risks & countermeasures in Information Systems
06th（11/04）	Guest Lecture
07th（11/11）	Security of individuals and society (1)
08th（11/25）	Security of individuals and society (2)
09th（12/02）	Midterm Presentation
10th（12/09）	Midterm Presentation
11th（12/16）	Cyber military superpower and its problem
12th（01/06）	Final Presentation
13th（01/13）	Final Presentation

Today's Topic

- Diversity of Risks & Risk Management
  - Countermeasures against risk
  - Risk evaluation/management
- Trade-off of Security Countermeasures
  - All security measures involve trade-off
  - Relationship with management

Diversity of Risks & Risk Management

10 major Security threats in 2009

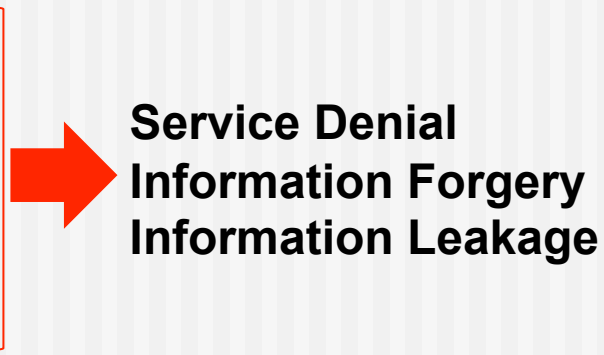
Attacking Techniques Become More and More Sophisticated

- Threats to Organizations
  - [1st] Threat of DNS Cache Poisoning
  - [2nd] Sophisticated Targeted Attacks
  - [3rd] Information Leakage Occurring on a Daily Basis
- Threats to Users
  - [1st] Diversified Infection Routes for Computer Viruses and Bots
  - [2nd] Threats Arising from Vulnerable Wireless LAN Encryption
  - [3rd] Never Decreasing Spam Mails
  - [4th] Threats Arising from Using the Same User ID and Password
- Threats to System Administrators/Developers
  - [1st] Threats of Attacks via a Legitimate Website
  - [2nd] Actualized Passive Attacks
  - [3rd] Potential Vulnerability in Embedded Systems/Devices

Ref: IPA Security Book 2009

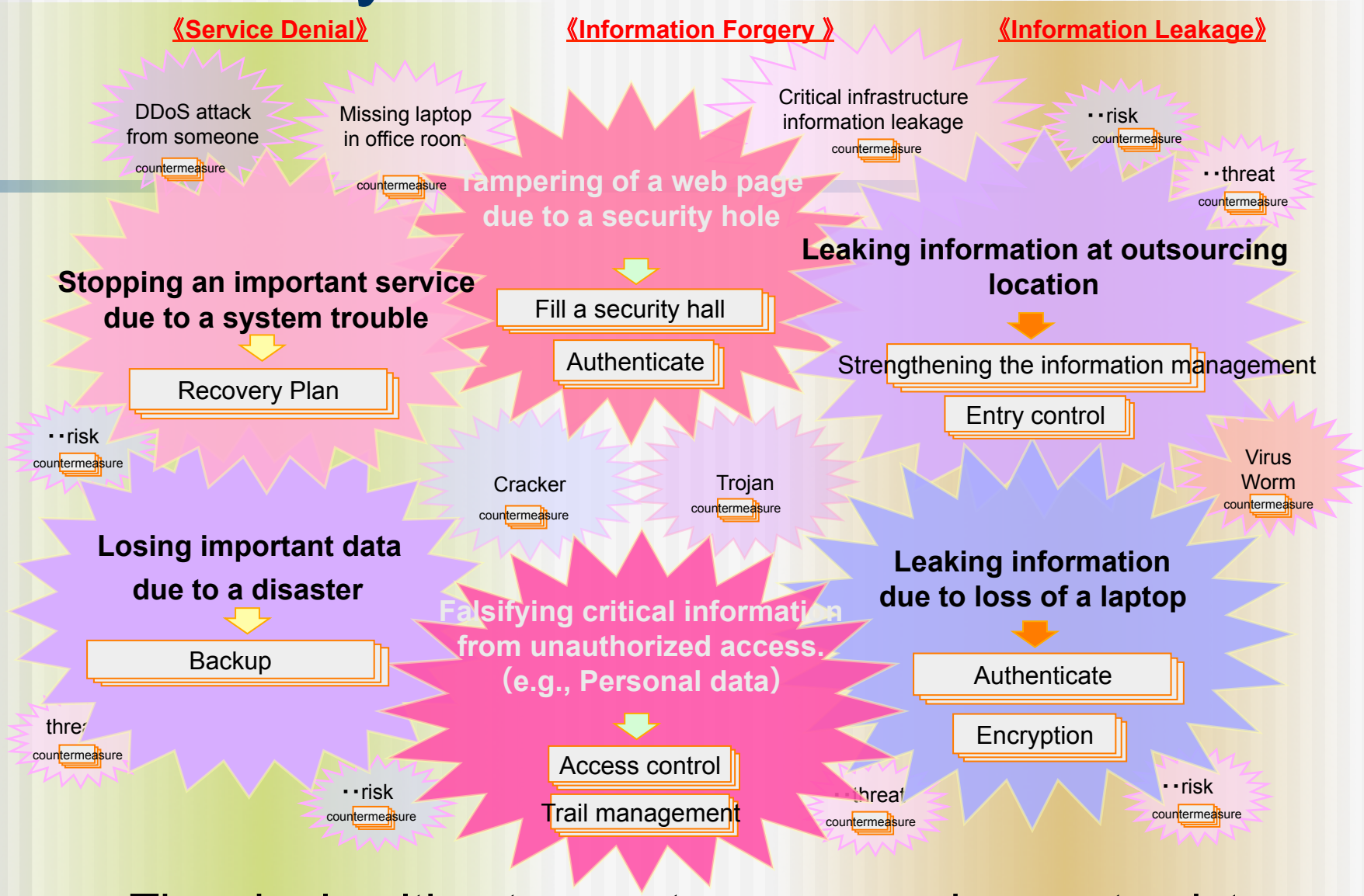
Trend of Cyber Attacks

- For Organization
  - Distributed Denial of Service
  - DNS Cache Poisoning
  - SQL Injection
  - XSS (Cross Site Scripting)



- For Individuals
  - Phishing
  - Spam
  - Targeted Attack

Diversity of Risks



The single ultimate countermeasure does not exist.
A countermeasure for each risk is necessary.

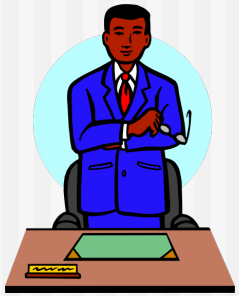
Exposure of a risk imposes significant impact on the company management

Leakage of confidential information

- Confidential information is managed on information system.
- Business know-how in the private sector, variety of sensitive information in government.
- Building trust

Leakage of personal information

- Leakage risk of personal information is expanding year by year.
- Once the outflow occurs, directly damages the business
- Not enough to apologize



Operational risk

- For stable and sustainable organizations, a stable system operation is needed
- To ensure business continuity, Information System is important
- Is not allowed to a organization, which doesn't work? (especially government)

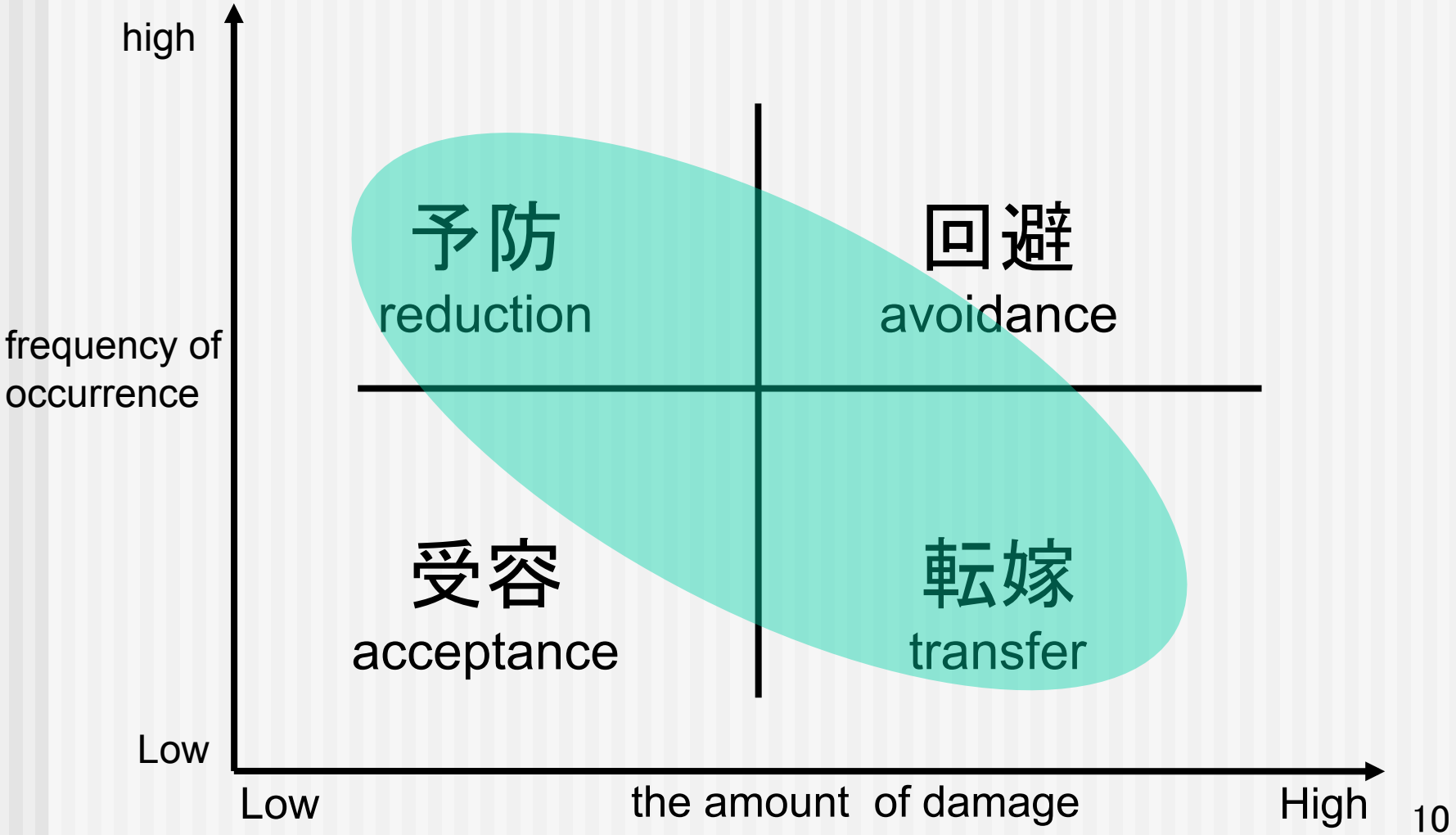
The impact on activity

- Experience, knowledge, or know-how are stored in Information system
- The environment in which effective cooperation between Information system and business is performed is needed.
- Business depends on Information system

Risk countermeasures

- What do we call risk?
  - Potential occurrence of a loss, damage, or any other negative things
  - Clarify risk frequency and its damage
- Risk analysis is the first step
  - What kind of risk factor does exist?
  - How often does the risk factor occur?
  - How large is the expected damage provoked by the risk factor?

Types of Risk Countermeasure



Risk evaluation

- Identifying characteristics of risks
  - Quantification of risks
  - What are characteristics of problems/risks?
- After quantifying risks (estimating expected damage), need to make decision on whether the risk is acceptable.
  - Risk assessment

Risk management

- The process to reduce/avoid frequency of risks,

  or any loss caused by a risk
  - Risk management tasks are executed when damage caused by a risk is not acceptable.
- To deal with a risk
  - Taking actions
    - Considering cost-effectiveness
    - Technical solutions
    - Protection by social system / legislations
- Points to be considered
  - Where do we perform a response? How do we perform it?
    - Is it reasonable?

Important Points on Risk Management

- Staying up-to-date
  - To manage a new risk
- Understanding Technology/Compliance
  - Technology is not perfect/Compliance is not absolute
- Identifying the characteristics of actions we can perform
  - Is it safety, not relief?
  - Does a new risk occur due to actions taken?
  - Do any risks remain?
  - Are costs of a response and a recovery plan reasonable?
- After understanding Technology/Compliance, consider a response and recovery plan based on both of them.

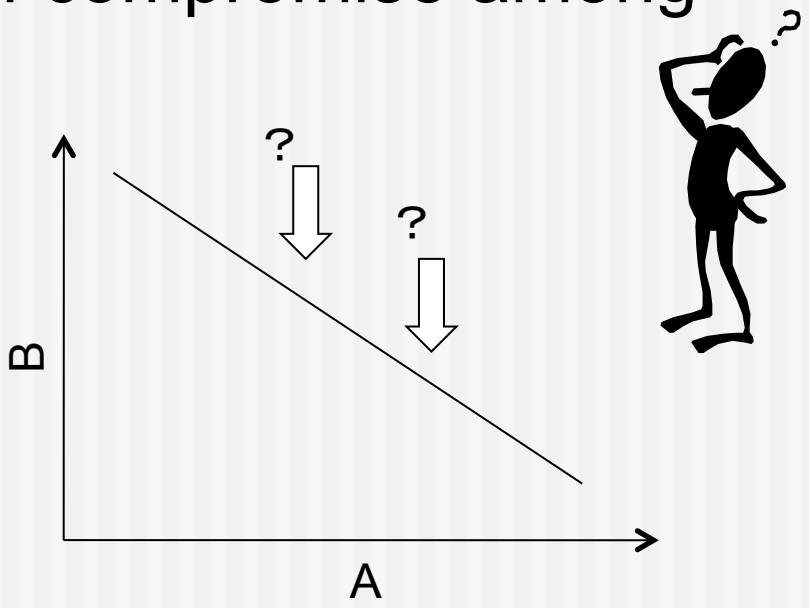
Trade-off of Security Countermeasures

All Security Measures Involve Trade-off

- Trade-off
  - All security countermeasures have merits and demerits
  - Concerning a risk countermeasure, are merits and demerits balanced?
- Advantages
  - Improving safety and reassurance
- Disadvantages
  - Human and economic costs (Initial, Operational)
  - Reduced usability
  - Occurrence of other risks

Relationship with Management

- Role of management
  - Make a selection among various security countermeasures
  - Decide one point of compromise among tradeoffs



Human and Economic Costs

- Initial costs
  - Buy and install products
  - Update and fix systems
  - Educate operators
- Operational costs
  - Maintain and upgrade systems
  - Stressed operators

Reduced usability

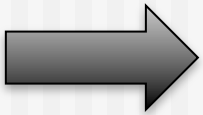
- Many security countermeasures reduce usability
  - Security check at boarding gates: making a long standing line
  - Web site filtering: inconvenience to everyone when accessing Wikipedia
  - Ban on using USB memory to prevent information leaking: difficulties to exchange data

Occurrence of other risks

- Unexpected risks may occur, caused by security countermeasures
  - Risks to break security countermeasures
    - Increase staff's risks of falling among, if biometrics are employed at banks and so on
  - Attacks using security countermeasure
    - Sending something illegal (drugs, guns)
  - Risks if security countermeasure faultily works
    - Filtering my blog site by trackback/comment

Selection of Security Countermeasures

- To what extent can we allow our security countermeasure to be costly and to reduce usability?
  - Can each stakeholder accept it?
  - Are cost and usability levels reasonable regarding risk?
- Is security countermeasure effective enough?
  - Do we sufficiently reduce the risk occurrence?
  - Do we suppress damage when the risk occurs?



Select security countermeasure by considering the trade-off balance

References

- Security Attacks
  - http://www.comptechdoc.org/independent/security/recommendations/secattacks.html
- BotSniffer: Detecting botnet command and control channels in networktraffic
  - http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.110.8092&rep=rep1&type=pdf
- 『セキュリティはなぜやぶられたのか』ブルース・シュナイアー著
  - 原著:”Beyond Fear”
- 情報セキュリティ入門　第4章
  - http://itpro.nikkeibp.co.jp/article/COLUMN/20060214/229302/
- 情報処理教科書 情報セキュリティスペシャリスト
- 情報セキュリティの課題と対応策
  - http://www.ssken.gr.jp/MAINSITE/download/newsletter/2009/20100120-stg-2/lecture-1/paper.pdf

2nd Assignment

第2回課題
攻撃の多様化と対策

- インターネット上のサービスについて、悪意あるユーザの攻撃により，重大な被害が発生した事例を調査し、その対策を提案してください。
- 注意点
  - 事例は有名なものに限らない。ただし、講義中に紹介した攻撃事例や，他の受講生 が既に取り上げている攻撃は除く。
  - 対策を述べる前に、かならず事例に関連するステークホルダを挙げること。
  - 対策を述べるときは、ステークホルダごとにどのようなトレードオフが発生するかを言及すること。
  - A4用紙 2枚程度にまとめ、SOIから提出すること。
- 提出期限
  - 取り上げる事例の報告 2010年10月30日(土) 23時59分
  - 課題レポート 2010年11月8日(月) 17時00分

2nd Assignment
Diversity of Risks & Countermeasures

- Concerning an internet service, survey the case of a malicious user attacking and seriously damaging the service and propose a countermeasure.
- Additional Information
  - A minor case will be fine. But do not pick cases introduced in the lecture or picked up by another student.
  - Before proposing a countermeasure, you must state the stakeholders related to the case.
  - When you propose a countermeasure, mention what are the trade-offs concerning each stakeholder.
  - Submit at most 2pages (A4) via the SOI webpage.
- Deadlines (JST)
  1. Picked up topic submission: 2010/10/30 (Sat) 23:59
  2. Assignment submission: 2010/11/8 (Mon) 17:00

Next Class

- Guest Lecture
  - 6th Class (November 4th)
  - Kazumasa Utashiro
    - Position
      - Fellow of Internet Initiative Japan
      - Administration Officer of JPCERT
  - Notes:
    We take a roll call in the day of guest lecture

Appendix

10大脅威　あぶり出される組織の弱点

- 1位　変化を続けるウェブサイト改ざんの手口
- 2位　アップデートしていないクライアントソフト
- 3位　悪質なウイルスやボットの多目的化
- 4位　対策をしていないサーバ製品の脆弱性
- 5位　あわせて事後対応を！情報漏えい事件
- 6位　被害に気づけない標的型攻撃
- 7位　深刻なDDoS攻撃
- 8位　正規のアカウントを悪用される脅威
- 9位　クラウド・コンピューティングのセキュリティ問題
- 10位　インターネットインフラを支えるプロトコルの脆弱性

出典:IPAセキュリティ白書2010

10 Major Security threats
Organizations' Security Flaws Brought to the Surface

- 1ST Ever-changing tactics for website defacement
- 2ND Client software not updated
- 3RD A variety of purposes/objectives of computer virus and bots
- 4TH Vulnerability in unsecured server products
- 5TH Information leakage without proper incident response
- 6TH Targeted attacks carried out without victims' noticing
- 7TH DDoS attacks that cause serious damages
- 8TH Unauthorized use of a legitimate account
- 9TH Security holes in cloud computing
- 10THVulnerability in protocol supporting the Internet infrastructure

Ref: IPA Security White Book2010

標的型攻撃 (Targeted Attack)

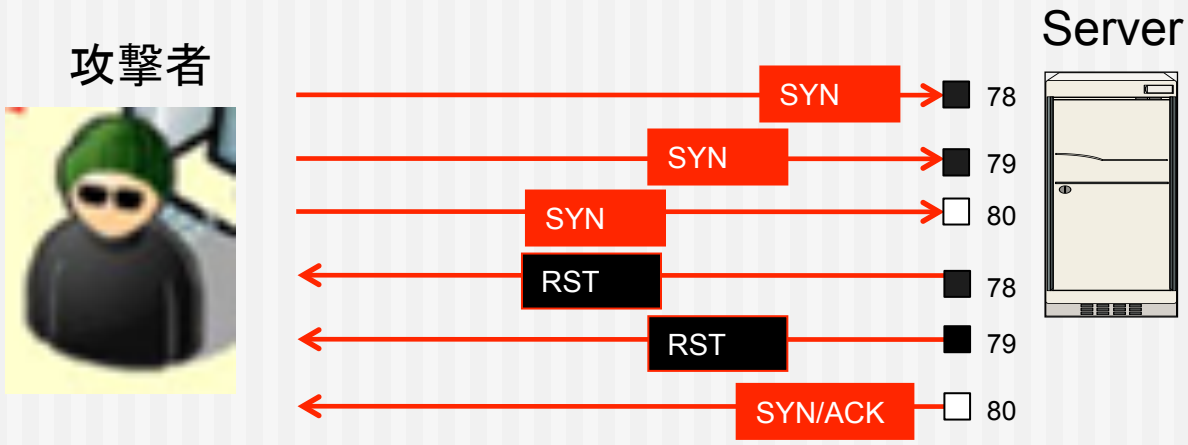
- 定義
  - 無差別に攻撃が行われるものでなく、特定の組織あるいはグループを標的とした攻撃
  - 攻撃対象となる組織あるいはグループに特化した工夫が行われる
- 種類
  - スピア型フィッシング
  - 標的型スパムメール
- Definition
  - Targeted attack focus on particular organization or group
  - This attack specialized to the each organization or group
- Type
  - Targeted phishing
  - Targeted spam mail

事例：防衛庁(現防衛省）関係者への攻撃
Case Study : Targeted Attack for the Japanese Defense Agency

- 2006年5月 (May, 2006)
- 対象 (Target)
  - 防衛庁関係者
  - Japanese defense agency officials
- 概要 (Overview)
  - 「時期防衛計画について」という件名のメールが大量送信
  - 防衛庁長官を装う
  - Large volume Mail that has title “Next Defense Program” was sent to the officials
  - This attacker pretended to the Director General of the Defense Agency

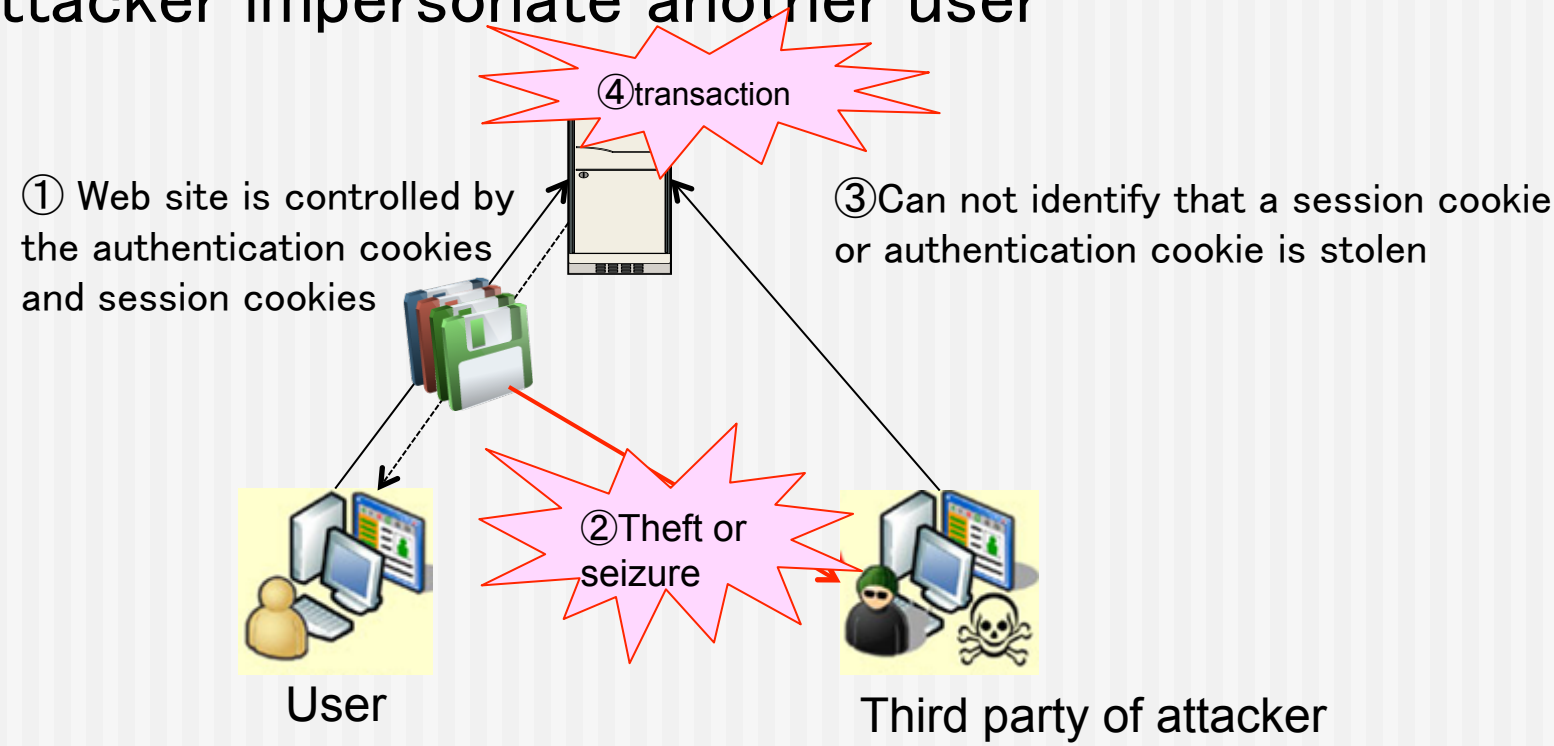
Port scan

- To look for available port in netwrok communication, Attacker sends a signal through a check

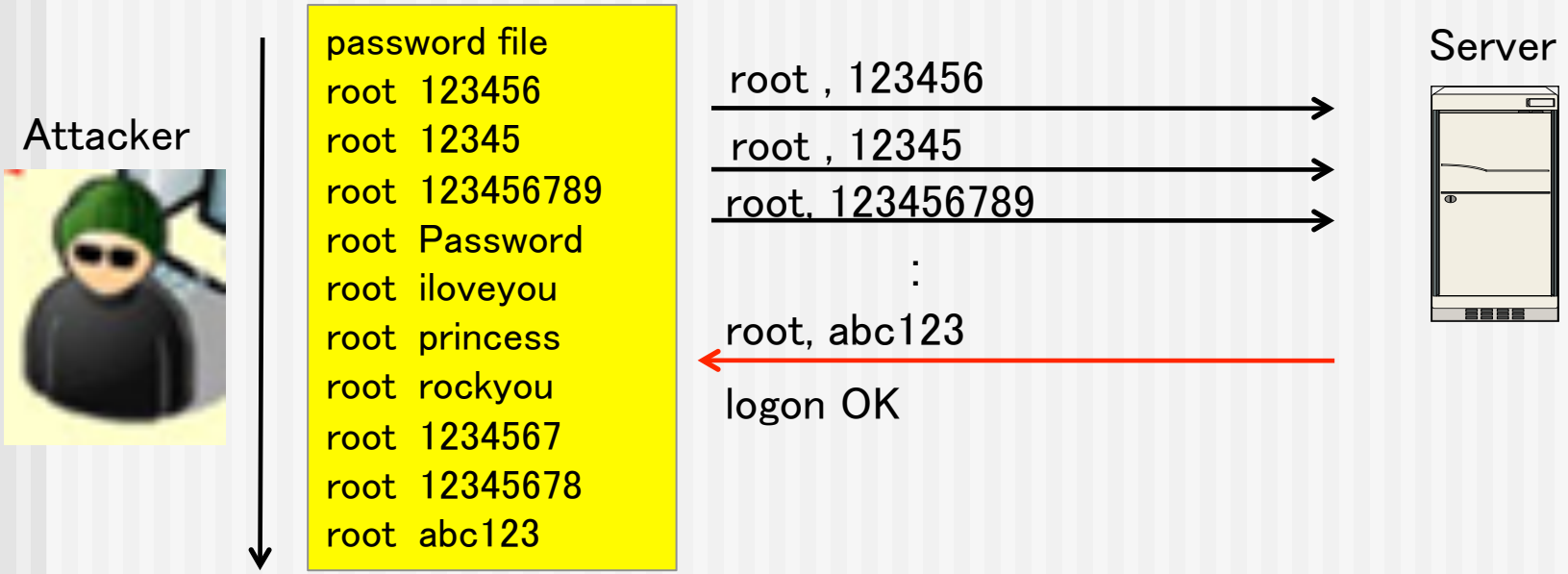


Session hijacking

- Stealing session ID and session・cookie ,
  Attacker impersonate another user



Password crack

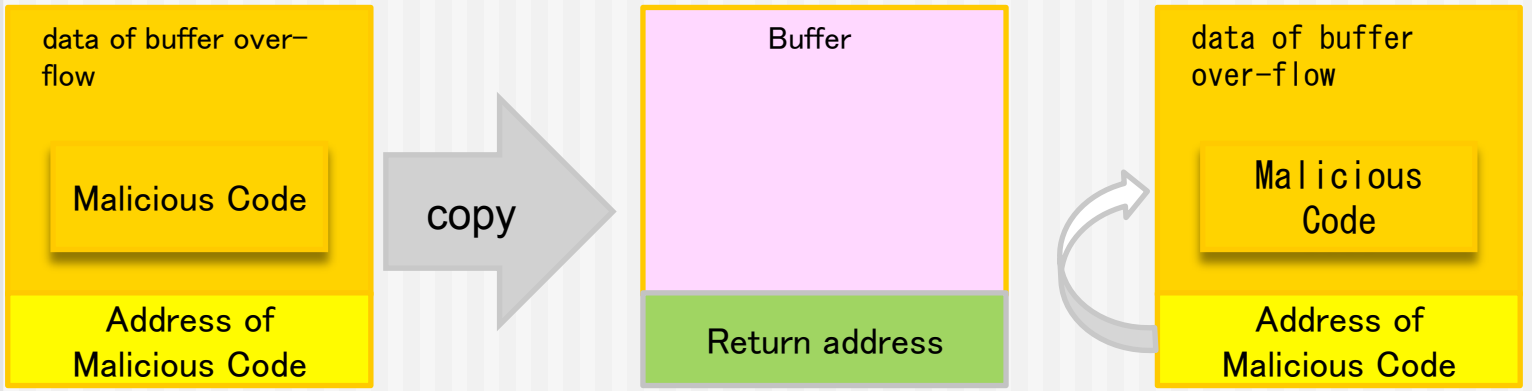


Buffer over-flow

Attacks targeting the vulnerability

strip target down of PC

target



Because of buffer over-flow,
Malicious code can be written instruction address of the function

WEBの脆弱性を狙った攻撃
XSS (Cross Site Scripting)

- XSSとは
  - 攻撃者が送り込んだ悪意のコード（Javascriptなど）を、そのページを閲覧した不特定多数のユーザーにスクリプトとして実行させる攻撃手法
- What is XSS?
  - Attacker makes web server deliver malicious script code (e.g. Javascript). This code execute in client's web browser and steal personal data in web application.
- 種類 (Type)
  - Reflected XSS
  - Stored XSS
  - DOM-Based XSS
- 対策：脆弱性の修正
  - トレードオフ：改修コストの増加

サービスに対する攻撃（DNS Cache Poisoning)

- DNS Domain Name System
  - ホスト名とIPアドレスを結びつける情報を提供
    e.g. www.example.com ⟷ 192.0.32.10
  - インターネットの基幹システム
    - DNSに依存したシステムが多い
    - DNS Cache Poisoningが企業内，ISPないで行われたら，どんな影響があるだろうか？
  - DNS translates computer hostnames into IP addresses
  - Internet mission-critical system
    - amount of internet system depend on DNS
    - What is an impact of DNS cache poisoning in a business network and ISP class network?
- DNS Cache Poisoningとは
  - ドメイン管理情報を書き換え
  - 特定のドメインに到達できないようにしたり、別のIPアドレスに誘導
- What is DNS Cache Poisoning?
  - This attack rewrites domain information