Security management in the Internet era

12th:Final Presentation
January 6, 2011

Jun Murai
Keio University

Suguru Yamaguchi
Nara Institute of Science and Technology

1

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 about 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

2

Assignment

- Pick up one of the greatest threats you think we urgently need to solve.
- Explain the reason you chose this threat and its impact in terms of technical aspects and damage.
- Enumerate the different stakeholders related to the threat and propose a "realizable" solution.

3

Supplementary Note

- The solution you propose must be explained in terms of both technical and social aspects.
- When considering the stakeholders involved in the implementation of the solution, classify them between the private sector and the government. In particular, make detailed propositions on the role of the private sector stakeholders.
  - Sum up concisely the solutions such as the enactment of a law
- Not only the domestic area but also stakeholders of the global community (foreigners, organizations, nations, etc.) should be considered.
- Concerning the proposed solution, give an account of its rationality based on risks, costs and trade-offs.

4

グループワーク課題

- 情報セキュリティにおいて，最も解決すべきだと思う脅威を具体的にひとつあげなさい
- なぜその脅威が最も解決すべき脅威なのか，どのような脅威であるのかを，技術面，被害のインパクトの面から説明しなさい．
- また，その脅威にかかわる人・組織（ステークホルダー）を分類し，" 実現可能な"対策を提案しなさい．

5

補足事項

- 対策は技術面と社会面の両側面から提案すること．
- 対策を実施するステークホルダーは民と官に分類して考えること．
  - ✓ 特に民の役割を詳細に提案すること．
  - ✓ 法律の制定などの行政による対策は，官の対策として簡潔にまとめること．
- 国内のみならず，国外の人，組織，国などグローバル社会のステークホルダーも考慮すること．
- 提案した対策について，リスク，コスト，トレードオフの観点から合理性を説明すること．

6

Schedule

- 6 Jan. Final Presentation
  - Group 1 and 3
- 13 Jan. Final Presentation
  - Group 2 and 4

7

Group 1

Code breakers in the future
一未来から解読者がやってくる

Group 1
Kazuki Matsuda, Keisuke Takemasa
Kyohei Moriyama, Tomokazu Wada
Shota Seo

What do you think?

- It is not possible to decode present encryptions in a moment.
  - 今日の暗号は、戦いの結果生まれた強固なものに見える
  - *WPA2, HTTPS, SSH, CDMA*
- But…
- Do you remember 10 years ago?
  - 10年前、何に安心して通信をしていたか覚えていますか？
  - WEP, TKIP…

Code (Encryption) – 暗号

- Encryption has its large history *more than 2000 years.* (about 40 times longer than the computer's history)
  - Peoples, Companies and Countries has fought as users or breakers of encryption all through the ages.
- 「暗号」はコンピュータの発明される前、紀元前から既に使われていた
  - 何千年もの昔から、王や女王や将軍たちは、国を治め、軍を動かすためには効率的な通信手段が不可欠であることを知っていた。それと同時に支配者たちは、メッセージが正当な受信者以外の手に渡ったり、貴重な秘密がライバル国家に奪われたり、重要な情報が敵の軍隊に漏れたりすればどうなるかもよく理解していたのである。 – サイモン・シン『暗号解読』

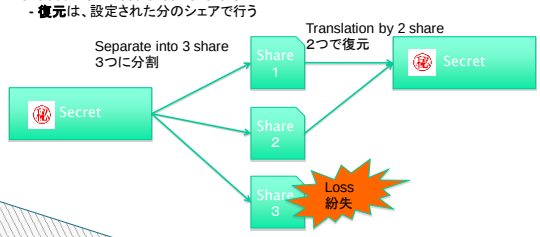
Abstract

- Protecting secrets except coding
  - 暗号化以外の秘密の保護
- Service of classing secrets by companys
  - 企業による秘密のクラス分けサービス
- Classing a way of coding by gavernment
  - 政府による暗号化方法のクラス分け
- Conclusion

  まとめ

Secret Sharing Scheme 秘密分散

- Separate distributed information (“Share”) → no mean !!
  - 機密情報を意味の無い分散情報(シェア)に**分割**
- Individual “share” don’t have any information
  - 個々のシェアからは、元の情報を類推不可
- Translation is in need of some “share”
  - **復元**は、設定された分のシェアで行う



Service of classing secrets by companies

- 民間企業が秘密をクラスわけし、ユーザにサービスを提供する。
- The private company classing divides the secret. And, it offers it as service.

Classing & Basis of selection

秘密のクラス分け(classing divides)

	説明	アクセス	対象
class A	最重要・極秘 Most Important・Strict secrency	経営層、最重要情報データ管理者 Management、Data Administrator	重要契約書、国税関係書類など Important contract, National tax document, etc
class B	重要・関係者外秘 Important・Concerned Only	業務担当者 Person in charge	顧客情報、人事関係書類など Customers Information, Human affairs document , etc
class C	社外秘 Inside Only	社内のみ Inside Only	営業情報、原価情報など Business information, Cost price,information etc
class D	一般 Normal	使用制限なし free	公開文書、一般的な資料など Open document, Normal document , etc

Classing & Basis of selection

秘密のクラス分け(classing of secret)

【クラス分け(重要度)の決定】Decision of Importance

①漏えいによる影響 Influence of Leakage
担当者の不正使用、担当者以外の社員、または外部からの不正アクセス、文書・媒体の複製、または持出し、盗難に関して、当該情報が漏えいした場合の信用の失墜、損害賠償、罰則の程度を考慮
Considering the level of confidence losing, compensation for damages, panel regulations in case of Illegal use, Unlawful computer access, Copy of document & medium.

②消失による影響 Influence of Disappearance
事故、不正操作、火災、天災等により当該情報が消失した場合、情報を適時に利用できない場合の影響を考慮
Considering the influence when information cannot be used at the right time, when information disappears by accident, all illegal operation, fire, and natural disaster.

③誤謬による影響 Influence of Error
過失、改ざん等により、情報に誤謬を生じた場合の影響の度合いを考慮
Considering the influence when error is caused by the fault and the falsification.

Classing & Basis of selection

【分類に応じた管理】Management according to classification

•分類に応じた管理方法や保管期限を明確にしておく必要がある。
•It is necessary to clarify the management method and the storage limitation corresponding to the classification.

•逆に、保管期限を過ぎた情報や重要でない情報を不必要なレベルで管理する可能性もある。煩雑な管理は情報セキュリティ担当者や利用者の負担が増すばかりで、情報の流通を阻害し、結果として管理が実施されないこととなってしまう可能性がある。
•Oppositely, there is a possibility of managing information that passes the storage limitation and information not important at a needless level, too. Complex management just increases the load of the person in charge of the information security and the user, and obstructs the distribution of information. There is a possibility not to be able to manage.

•なお、情報はクライアントの状況や時間の経過などに応じて、その重要度が変化することがある。したがって、一度分類した管理を固定するのではなく、定期的に見直す手続きが必要である。
•The importance changes into information according to the passage of the situation and time of the client. Therefore, the procedure reviewed the management classified once is not fixed but regularly is necessary.

Service of classing secrets by the government

- 未来の解読者から見たら、現代の暗号化は簡単に解読出来る…しかし、現代人にこれを防ぐ手だてがない…
- The people in the future have a special skill, so the people in the present can’t prevent them.

- 政府が事前に暗号化技術のクラス分けを行う…解読された時の企業の過失について考える手助けとして、暗号化ごとにクラス分けを行う。

→現段階における暗号化技術を評価する！

- The government classify the cryptography for an indicator.

Classify cryptography

Class	Cryptography
Class A	DES,
Class B	AES,IDEA
Class C	RSA, Triple DES,楕円曲線暗号 (Elliptic curve cryptography)

- 3つのクラスに分割…Class A, B, C の順に暗号化強度が高くなる。
- Classify cryptography into 3 class
- Cipher strength is strong in alphabetical order

- Class A による過失は重度のもので,Class Cによる過失は企業側の責任は問われないものとする。
- Negligence of class A is very serious , but Negligence of Class C is no serious for the company

Problem

- 暗号化技術だけに基づいて判断するのか？
  - 情報の管理体制(ハード・ソフト面)も考慮する。
- The point of negligence is only cryptography?
  - That is considered about hard and soft.

- 誰が判断するのか？
  - 官・民双方からの有識者を募り、2つの側面から企業の過失を判断する。
- Who judge?
  - 2 angle. Companys and the government

まとめ

- We suggested secret sharing scheme
- 暗号化以外の手法として秘密分散を提案
- Companies provide secret class for users
- 企業が秘密の度合いわけをユーザへ提供
  - Users can choice secret protections matching up to their secret class.
  - ユーザは秘密の度合いに合った保護を選択可能
- Gavernment decides which code should be used
- 政府が暗号を使わなければならないか決める

Discussion

Group 3

SECURITY UPDATE

Shota Nagayama
Takatoshi Kanazawa
Ryosuke Imayoshi
Shinya Kanda
Sig2010-g3@soi.wide.ad.jp

問題 Problem

- セキュリティアップデートの標準化
  Standardization of Security update for users and ve
- 問題 Problems

ユーザ / User	・マニュアル操作 manual update -（知識不足、アプリケーション過多により）大変 difficult, by lack of knowledge and too many applications ・意図しないタイミングでのアップデート autoupdate, undesirable timing
ベンダー/Vender	・セキュリティアップデートはコスト高 Security Update matters cost high

Need to make smart these situations.
このあたりをスマートにしたい。

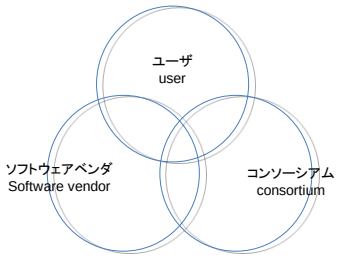
シナリオscenario

- アップデートしないとき when not update
  - ①脆弱性をついた攻撃 vulnerability issue
  - ②感染 infection
  - ③発病そして伝染 attack and infection
  - ④情報流出 flow of information
- アップデート行わないと大変なことに！！ It grows serious if it does not update

アップデートの方法
update method

- 既知（公開された）の脆弱性の対策 countermeasures of the public vulnerability
- 情報弱者への対策 countermeasures of the users
- 対象外 out of scope
  - 使っていないパソコンのアップデート update of PC that doesn't use it
  - 情報技術に長けている人 for specialist

ステークホルダー
stakeholder



コンソーシアム
consortium

- ソフトウェアベンダを軸に構成 organized by software vendor
- 運営などは公募により決定 administrator is publicly seek
- OSごとにアップデートのやり方の検討 How to update the every OS

特殊環境

- クラウド
- 組み込み機器

クラウド環境におけるソフトウェアアップデート
Software Update Mechanism in a Cloud Environment

- 想定環境 / Environmental Assumptions
  - SaaS等，ソフトウェアの実態がサーバサイドに存在する形態 / Service providing architecture where the actual software logic resides inside a remote server where the user would access through a client interface
- アップデート対象 / Target Required for Software Update
  - サーバサイド：プログラムのロジックやDBを含む器官部分 / Server side : Core software component which encapsulates core components such as the program logic and database
  - クライアントサイド：サーバサイドへアクセスするためのインタフェース / Client Side : Client interface to access the server side architecture
- 提案 / Our Proposed Solution
  - SaaSにおけるサーバ・クライアント間のインタラクションにおける規定を設ける / Provide a regulation for server and client side interaction under such environment
  - サーバサイドのロジックに関しては，ソフトウェア提供ベンダ毎に本発表における提案手法による解決を目指す / Apply the software updating scheme discussed through this presentation for server side architectures

クラウド環境におけるupdateの考察

クラウド管理者 (Administrator)	エンドユーザ (End User)
サービス (Services) ・	ブラウザ (Browser) ・

クラウド環境におけるupdateの考察

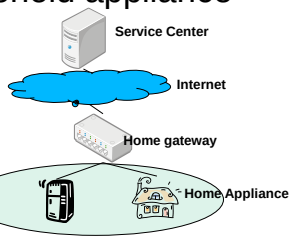
クラウド管理者 (Administrator)	エンドユーザ (End User)
サービス (Services) ・updateは容易 (easy to update) ・servicingとupdatingの並列化 (paralleling servicing and updating)	ブラウザ (Browser) ・updateは容易 (easy to update) ・update対象は1つ (only one target to update)

クラウド環境におけるupdateの考察

クラウド管理者 (Administrator)	エンドユーザ (End User)
サービス (Services) ・updateは容易 (easy to update) ・servicingとupdatingの並列化 (paralleling servicing and updating)	ブラウザ (Browser) ・updateは容易 (easy to update) ・update対象は1つ (only one target to update)

クラウド環境はupdate問題への耐性を持っている。
Cloud system itself is robust against update-problem.

家電/A household appliance



提案
ホームゲートウェイの導入
- ファームウェアの自動ダウンロード
- /An automatic download of the firmware
- 機器未使用時の自動アップデート/
- Automatic update in mint condition
- 一家に一台情報家電管理ホストを置く
- /1 install one information household appliance management host in the house
  - ホームゲートウェイとして普及させる

家庭内に情報家電が接続された際には自動認識，未使用時に自動アップデート

おしまい

Background:Security update problem

For users

- Difficulty
  - Lack of knowledge of the security menace
  - Overdoing of the installation software
- Troublesome

⇒The problem of the feeling, Therefore this problem is difficult

For vendors

- The Security Update has high cost
  - The reduction of the update's cost

We propose Security update standardization for users and vendors

38

About security update

- To prevent the damage from malwares on the Internet
  - To prevent the leak of the personal information
- Install a patch filling the security hole of the software
- After a notice from the software vendor, most are performed by the manual operation of the user

39

Frequency of the update

- Acrobat Reader
  - Update it once one ~ two months
- Thunder Bird
  - Update it once one week~ two months
- FireFox
  - Update it once two weeks ~ a month

→When the number of software in the PC increases, you must patch it frequently

40

The damage when we neglect update

- Phishing
  - An information leak
    - A credit card number
    - 2006:A yahoo auction phishing case
      - The number of victim is more than 700 people,and total damage reached100,000,000 yen
- A PC is taken over; Bot
  - we trouble another person,if we are infected with a computer virus
  - Virus infected computers could be used as a relay node by criminals for multiple malicious uses

The person himself does not notice it

41

The reason that we do not update

- Difficulty
  - Lack of knowledge of the security menace
  - Overdoing of the installation software
- Troublesome

⇒The problem of the feeling, Therefore this problem is difficult

42

Security holes we focus

Users running unpatched software are security holes.

- Machines owned by such people can be attacked
- Actually, security update itself enlarges the necessity of security update
  - It does not only save us from incidents but also broadcast the vulnerabilities it patches to crackers

Problem definition

what to update

- OS
- Application
- Firmware etc...

Existing updating method

- windows update
- Mac Software Update
- Think Vantage etc....

Problem definition

what to update

- OS
- Application
- Firmware etc...

Existing updating method

- windows update
- Mac Software Update
- Think Vantage etc....

Anyway, all programs connected to the network needs to be updated.

Problem definition

what to update

- OS
- Application
- Firmware etc...

Existing updating method

- windows update
- Mac Software Update
- Think Vantage etc....

Anyway, all programs connected to the network needs to be updated.

What's the problem?

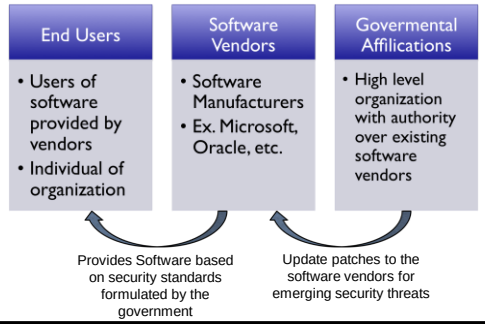
- The way to update is different, depending on each vendor.
-- needs many time
-- needs many learning

- Are they really patches all the vulnerabilities the we know?

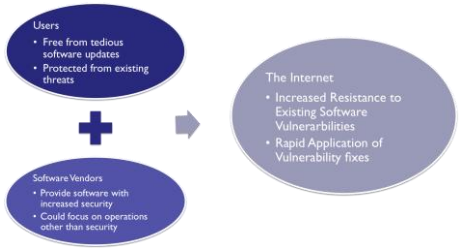
What we can do?

- Standardize the security update
  - We can simplify it for unlearned people
  - We can bring the interfaces/methods together into an interface/method

Stakeholders



Merits



Stakeholders Involved in Standardization

- Vendors
  - Create software based on government standards
- Government
  - Provides a universal standard for all software to avoid security issues
  - Standards are updated dynamically for emerging security issues
  - Check vendor software for compliance

Problems

- Cost
  - High Starting Cost for Software Vendors
  - Requires Refactoring of Existing Software
- Trust
  - Has higher institutions enough trust / technology / knowhow / manpower, for software vendors to blindly entrust it's software's security issues to the government?
- Responsibility
  - Very, very high risk for the government if something goes wrong

Technical problem of the standardization

- Government needs high IT-skill
  - When make standard, patch and find security hole
- Standardization make security hole
  - Have to stonewalling defense
- How do we generate the security patch
  - We want to make automatically
- How shall we deal with systems which are already
  - Some systems cannot be stopped
- Some systems don't run when update the software
  - System can run designated software version

52

Solution

- Simplified update rule
  - Make protocol to manage update
  - Implementation
    - Application, OS, Farm ware
- Government makes software to manage

53

Lower stress method

- Actual condition
  - Have poor support
  - Get caught in the crossfire
- Standardization case
  - Security in one position
  - User friendly

54

Epilogue

- We focused on software update
  - OS, Firm ware , Application
- We propose software update standardization
  - Support to multi platform
- It is ideal to standardization is bureaucracy-led system
- Urgent countermeasures are required by vulnerabilities

55

Thank you for listening

56

Discussion

Schedule

- 6 Jan. Final Presentation
  - Group 1 and 3
- 13 Jan. Final Presentation
  - Group 2 and 4

58