オペレーティングシステムのセキュリティ機能
--- 韓国光州科学技術院との国際調査研究---

櫻井 幸一
九州大学大学院システム情報科学研究院

（PPT edited by 田端 利宏[岡山大]
Updated in 7th June 2005

発表手順

1. プロジェクト全体の説明（プロポーザルの説明）
2. 活動概要
3. 共同研究の内容と成果
4. アンケートの結果
5. 韓国の ITRC 紹介
6. 韓国でのOSセキュリティ技術の研究の歴史と動向
7. 組み込みシステムのセキュリティの必要性
8. OSセキュリティの調査結果
9. おわりに

プロジェクト全体の説明

- 調査研究のテーマ
  - オペレーティングシステムのセキュリティ機能に関する調査研究
- そのテーマの戦略的意義／位置付け
  - 不正侵入や個人情報の漏洩が多発
  - 計算機システムのセキュリティの向上が必要
  - 計算機の基盤ソフトウェアである OS
    - SELinuxに代表されるセキュアOSへの注目
    - IDSやバッファオーバフロー防御技術など
- セキュアOSの研究において，日本よりも長い歴史と経験を有する韓国の研究者（Gwangju Institute of Science and Technology（GIST））と連携し国際共同研究

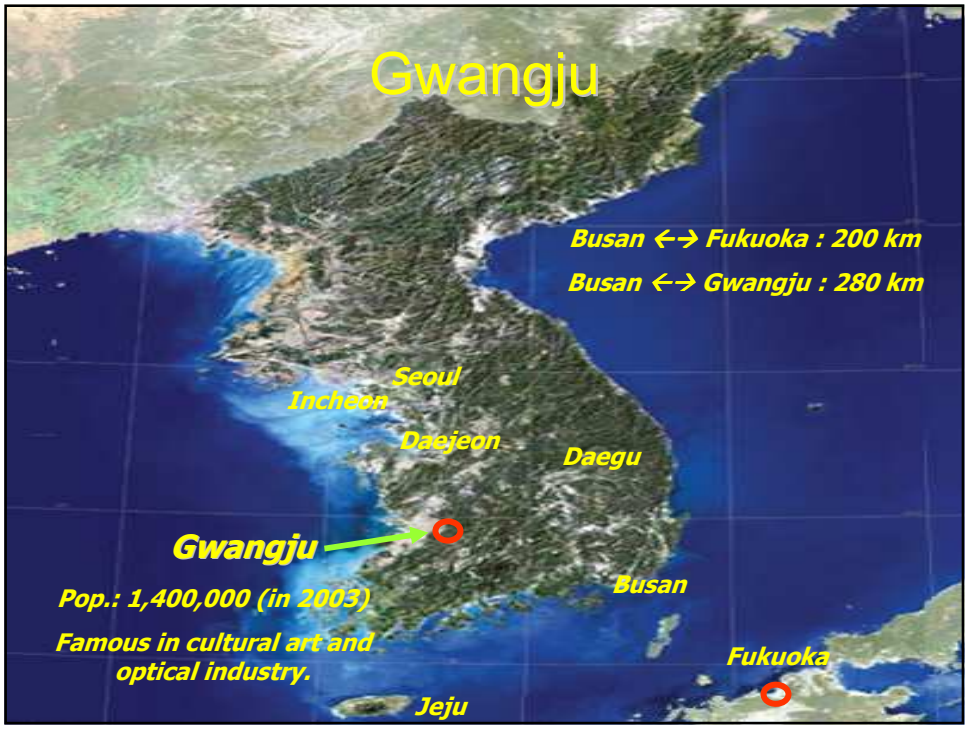
構成メンバー

- 大学（6名）
  - 櫻井 幸一 （九州大学，教授，本プロジェクトの主査）
  - 田端 利宏 （九州大学，助手，（現在，岡山大学助教授））
  - 鑪　講平 （九州大学，M1）
  - 長野　文昭 （九州大学，B4）
  - R. S. Ramakrishna（GIST，Professor）
  - Wook SHIN（GIST, Ph.D candidate）
  - Hyung Chan KIM（GIST, Ph.D candidate）
  - Ji Ho Cho（GIST, M2）
- 企業（5名）
  - 櫻庭 健年 ((株)日立製作所システム開発研究所)
  - 進 博正 (株式会社東芝　研究開発センター)
  - 藤田 卓志 (株式会社富士通研究所)
  - 宗藤 誠治 (日本アイ・ビー・エム株式会社、東京基礎研究所)
  - 森尻 智昭 (東芝ソリューション株式会社　SI技術開発センター)

Security Research Group/GIST

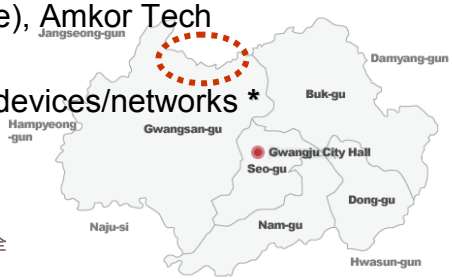
Security Research Group
Dept. of Information and Communications
Gwangju **I**nstitute of **S**cience and **T**echnology

（PPT edited by Hyung Chan Kim）



GIST in High Tech Complex

- High Tech Complex, Gwangju city
  - **GIST**
  - ETRI (Optical Communications Research Center) *
  - Advanced Photonics Research Institute *
  - Korea Photonics Technology Institute *
  - SAMSUNG (Home appliance), Amkor Tech (Semiconductor)
  - Several ventures on optical devices/networks *



光州

SSR-2005 全

GIST Scenery

Summer of GIST

*. Bldg. C of Info. & Comm. department in where our research group reside

SSR-2005 全体報告会

No.8

GIST !?

http://www2.gist.ac.kr/

- Gwangju Institute of Science and Technology
  - Founded in 1995
  - Government funded graduate school.
    - Ministry of Science and Technology (MOST)
    - In Korea, two MOST funded Univ.: GIST and KAIST
  - Scale
    - Five departments toward fusion technology
      - **Information and Communications**
      - **Materials Science and Engineering**
      - **Mechatronics**
      - **Environmental Science and Engineering**
      - **Life Science**
    - 69 regular professors
      - Including 6 foreign regular, excluding 22 foreign research prof.
    - 700 students (including 70 foreigners)

GIST !?

- Top 5 graduate school in science and technology in Korea
- Research & Education
  - Worldwide excellence
    - Optical Networks, Life Science, and Environmental Science
  - Education
    - 1.44 lectures per one faculty
    - All lectures are given in English (For the first time in Korea)
    - Total exemption from expenses for all students
    - Military replacement for the PhD course by law (only GIST and KAIST)
  - Publication
    - First rank in SCI journal publication per one faculty in Korea since 2001 – current.
      - **GIST(5.46),** POSTECH(4.32), KAIST(3.20), SNU(2.96) in 2003.
      - Average 6.4 journals per one Ph. D. course in 2005 graduation.
  - Research fund
    - First rank in fund scale per one faculty in Korea since 2001 – current
      - **GIST(5.6),** ICU(3.74), POSTECH(3.24), KAIST(2.92) in 2003. (Billion KRW)

Information and Communications Dept.

http://infcom.gist.ac.kr/

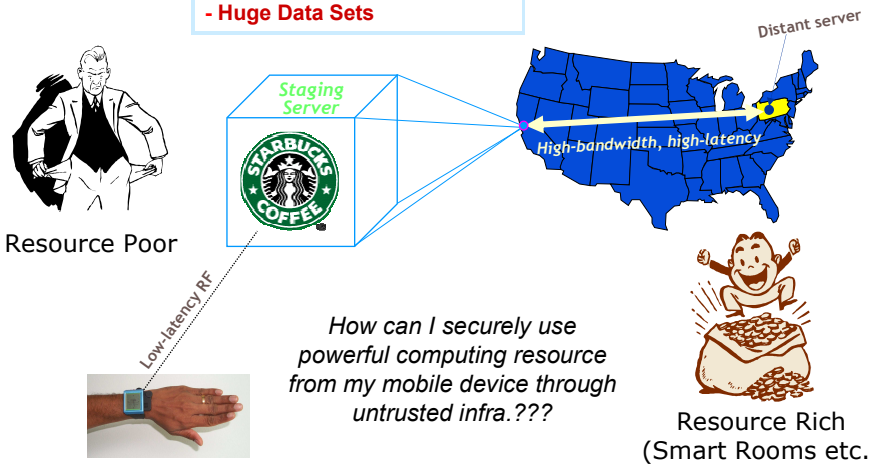
- Two research divisions
  - **Photonics & Semiconductor Device**
    - Quantum Integrated Photonics Lab
    - Specialty Optical Fiber Technologies Lab
    - Laboratory for Fast Optical Information Processing Technology
    - Photonic Device Measurement Lab
    - Applied Optics Lab
    - Optical Fiber Device Lab
    - Optoelectronics Lab
    - High Speed Integrated Circuit Lab
    - Microwave Optoelectronics Group
  - **Multimedia & Information System**
    - Multimedia Communication System Lab
    - Visual Communication Systems Lab
    - Optical Communication Lab
    - Speech, Audio, and Language Communications (SALC) Lab
    - **New Wave Computing Lab**
    - UbiComp and Virtual Reality Lab
    - Networked Media Lab
    - Communication System Lab

Security Research Group

- The team: SeeCure (since 1996)
  - ***SeeCure !? = See + Cure***
    - See: watch or investigate malicious actions
    - Cure: protection or safeguard
  - 1996-2003, **C**oncurrent **S**ystems **R**esearch **L**aboratory.
  - 2004-current, part of **N**ew **W**ave **C**omputing **L**aboratory.
- Main Research Themes
  - Workflow Systems, Home Networks based on Mobile Agents, Pervasive (Surrogating) Computing (1996-2003)
  - Trusted Operating Systems and Model of Access Control (2000-current)
  - Security Protocols for Distributed Sensor Network (2004-current)

Surrogating (Virtual Private) Computing

- Resource intensive App
- Huge Data Sets



Mobile Code Security

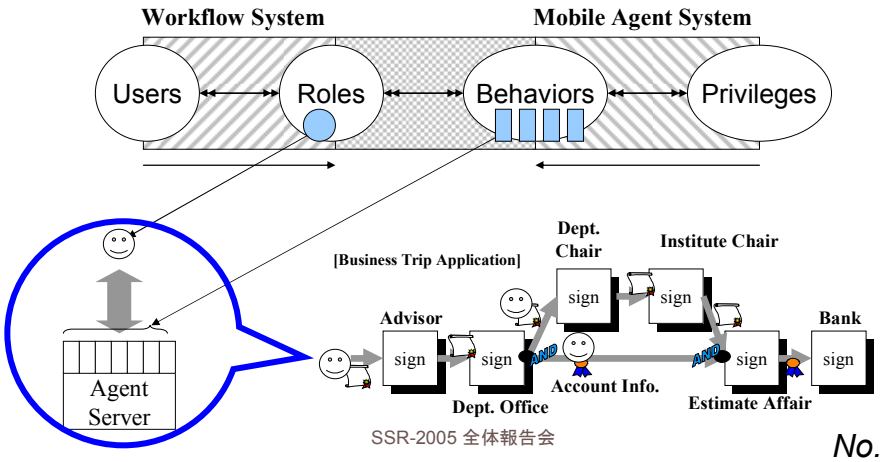
- *The protection of mobile agent from malicious agent server*

	Integrity	Confidentiality
Agent Code	✓	✓
Agent Data	✓	✓

One-time Agent Key

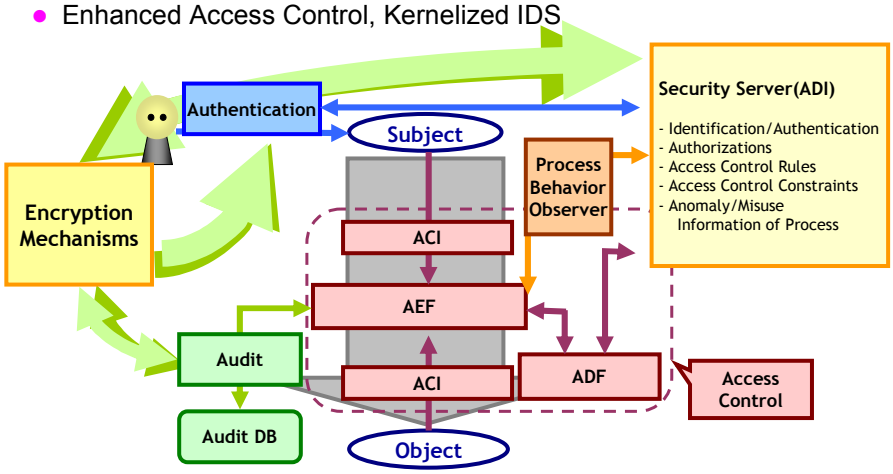
Mobile Agent based Workflow Management System

- A Layered Approach : Role-Behavior Based Control



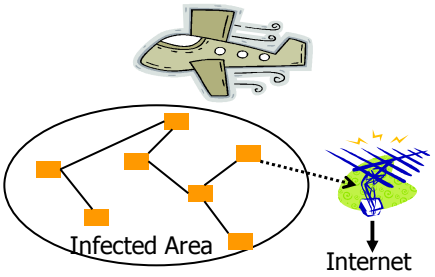
Trusted Operating Systems

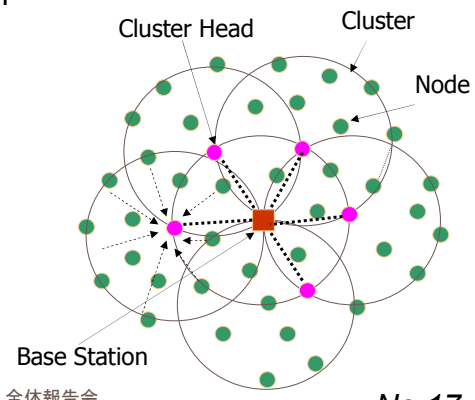
- SeeCure OS (Themis Kernel Architecture)
  - Enhanced Access Control, Kernelized IDS



Distributed Sensor Networks

- Light Weight Key Management
- Pairwise Key Distribution
- Dependable Routing Algorithm
  - Secure Cluster Routing
  - Energy Efficient Routing





Project

- *Secure Routing for Distributed Sensor Network*, GIST, (2005)
- *A Survey of Distributed Sensor Network Security*, GIST Center for Distributed Sensor Network, (2004)
- *A study on trusted embedded OS and its formal verification*, Ministry of Information & Communication (2004)
- *Formal Methods for Security Verification of Secure OS*, National Security Research Institute (2003)
- *A Study on Protection Mechanism in Java*, National Security Research Institute (2002)
- *A Secure OS Development*, Ministry of Information & Communication (ITRC) (2000-2002)
- *A Survey on Intrusions and Vulnerabilities*, Secuve CO, Ltd., Korea (2000)
- *Development of Secure Digital Transaction Systems*, Ministry of Commerce, Industry & Energy, and Giga Tech. Co, Ltd., (2000-2001)
- *KHF 2002: The 1st K-JIST Hacking Festival*, GIST BK21 (2002)
- *KHF 2003: The 2nd K-JIST Hacking Festival*, GIST BK21 (2003)
- *Hanuri/TFlow 2.0: Workflow Process Tools Development*, Electronics & Telecommunications Research Institute (1999-2000)
- *A Mobile Agent based Workflow System*, Electronics & Telecommunications Research Institute, and Korea Science & Engineering Foundation (1999-2000)

Advisors of Security Research Group

- **(Former) Prof. Dong Ik LEE** **1996-2003**
  - Ph. D. in Osaka University, (Under Prof. Sadatoshi KUMAGAI)
  - 1995-2003, Assistant, Associate, and Full Professor of GIST
  - 2003, Dean of Dept. of Info. & Comm., GIST
  - Member of IEEE, ACM, IEICE, KISS, KIPS, KIISC
  - Research Interests:
    - Petri Net Theory, Concurrent Systems Design
      VLSI Hardware Design, Mobile Agent, Information Security

- **Prof. R. S. Ramakrishna** **2004-current**
  - Ph. D. in Indian Institute of Technology (IIT), Kanpur, India
  - 1980-1995, Assistant, Associate, and Full Professor of IIT, Bombay
  - 1996-current, Professor of GIST
  - Member of IEEE, ACM
  - Research Interests:
    - Computer Graphics, Distributed and Parallel Computing, Quantum Computing
    - Many areas of Theoretical Computer Science

Members

- **Dr. Jong Youl PARK**
  - Ph. D. in GIST, 2004
  - 2004-current, ETRI
  - Research Interests:
    - Cryptography, Authentication, Mobile Agent Systems
      Pervasive Computing, Home Networks

- **Dr. Wook SHIN**
  - Ph. D. in GIST, 2005
  - Visiting Scholar in Univ. of Illinois Urbana-Champaign
  - Research Interests:
    - Model of Access Control, Trusted Operating Systems
      Formal Verification (Petri Net Model)

Members

- **Mr. Jung Min KANG**
  - M.S. in GIST, 2002
  - 2002-2003, SAMSUNG SDS
  - 2003-current, National Security Research Institute
  - Research Interests:
    - Access Control Model (BLP), Trusted Operating Systems

- **Mr. Hyung Chan KIM**
  - Ph. D. candidate since Sep. 2003
  - Research Interests:
    - Access Control, Trusted Operating Systems Program Security, Distributed Systems Security

Members

- **Mr. Ji Ho CHO**
  - Ph. D. student in Mechatronics since 2005. (Moved)
  - Research Interests in his master course:
    - Trusted Operating Systems, Cryptographic File-systems
- **Ms. So Young PARK**
  - 3rd semester of MS course
  - Research Interests: Distributed Sensor Network
- **Mr. Keyong Tae KIM**
  - 2nd semester of MS course
  - Research Interests: Distributed Sensor Network
- **Mr. Seog Chung SEO**
  - 1st semester of MS course
  - Research Interests: Distributed Sensor Network

Mr. KIM, Hyung Chan

Email: kimhc@gist.ac.kr
URL: http://www.seecure.org, http://nwcl.gist.ac.kr/~seecure

Phone: +82 62 970-2291 Fax: +82 62 970-2204

Security Research Group, NWCL, Dept. of Info. & Comm.
Gwangju Institute of Science and Technology
1 Oryong-dong Buk-gu, Gwangju, 500-712, Rep. of Korea

共同研究提案の背景@2003年度

- 2003年12月22日: 研究交流セミナー
  - 場所:光州科学技術院
  - 参加者:田端, 許, 鑪(九州大学から3名),
    光州科学技術院から5名, NSRIから2名
  - 光州科学技術院の発表は2件, 九大側の発表は3件
- 2004年3月19, 20日 : セキュアOSセミナー
  - 日時 :2004年3月19-20日
  - 場所 :韓国 光州科学技術院
  - 参加者:光州科学技術院(7人), NSRI (2人), 九州大学(4人)
  - 光州科学技術院の発表は3件, 九大側の発表は2件

韓国の政府系研究機関

- KISA (IPA@日本)
- ETRI　(CRL/NICT@日本)
- NSRI　(NSA@米国)

活動概要

- 打ち合わせ
- 共同研究
- 国際会議での動向調査
- 国内会議での動向調査
- 合同セミナー
- 最新研究動向の調査
  - 組み込みシステムのセキュリティ
  - アクセス制御機構
  - 侵入検知システム
  - バッファオーバフロー対策
- 韓国でのセキュアOSの研究動向調査
- 研究情報源の収集

打ち合わせ

- 研究調査の方針決定や意見交換，成果報告を目的として3回打ち合わせを行った
- 2004年9月9日（木） キックオフミーティング
  - 九州大学東京オフィス
  - SSR事務局 佐藤さま参加
- 2004年10月19日（火） 打ち合わせ
  - 東芝＠浜松町
- 2005年 1月 24日（月） 第3回打ち合わせ
  - 富士通研究所＠明石
  - IPA 宮川さま参加
- 2005年4月26日（火）
  - 東京プリンスホテル
  - SSR事務局 佐藤さま，内閣官房 青木さま，IPA 宮川さま参加

共同研究の内容と成果

- セキュアOSについて共同研究
  - 課題
    - Extended-Role Based Access Control
    - Privilege Transitional Attack
    - Data Protection on Ext3 File System
  - 成果
    - 国内会議での発表（CSS2004, SCIS2005）5件
    - 電子情報通信学会論文誌（論文1件，レター1件）
- 博士論文
  - 博士論文の執筆についても指導を行った

博士論文指導(副査)

- **Dr. Jong Youl PARK**
  - Ph. D. in GIST, 2004
  - 2004-current, ETRI
- **Dr. Wook SHIN**
  - Ph. D. in GIST, 2005
  - [will be]Visiting Scholar
    in Univ. of Illinois Urbana-Champaign

国際会議での動向調査(4件)

- 13th USENIX Security Symposium
  - (August 9-13, 2004, San Diego, CA USA)
- 1st International Conference on E-business and Telecommunication Networks (ICETE2004)
  - (August 25-28, Portugal)
- 9th European Symposium On Research in Computer Security (ESORISC2004)
  - (September 13-15, 2004, French Riviera, France)
- Seventh International Symposium on Recent Advances in Intrusion Detection (RAID2004)
  - (September 15-17, 2004, French Riviera, France)

国内会議での動向調査（5件）

- セキュアOS カンファレンス
  - (December 6, 2004, 東京品川,)
- 暗号と情報セキュリティシンポジウム 2005
  - (January 25-28, 2005, 兵庫県神戸市)
- 情報処理学会第67回全国大会(電通大)
  - (March 2-4, 2005, 東京都調布市)
- 第28回CSEC研究会(大阪大学)
  - (March 22-23, 2005, 大阪府吹田市)
- 第3回 セキュアOSカンファレンス
  - (May 13, 2005, 東京都)

合同セミナー

- 2004年7月に九州大学において開催した
- その場でそれぞれの研究課題について意見交換を行った
- プログラム

[Mobile Authentication]
- B. Cha: Location Information for Roll-Call System via Cellular Phone

[Protocols]
- K. Imamoto: Design and Formal Verification of Secure Cryptographic Protocols

[Auction]
- Y. S. Her: Electronic Sealed-Bid Auction with Efficient
- Communication Complexity Using Tournament Opening Method

[PKI]
- S. Koga: Efficient Pre-production Methods in Online Certificate Status Protocol

[RFID]
- J. Saito: Enhancing privacy of Universal Re-encryption scheme for RFID tags

合同セミナー（続き）

[Operating system]
- H. C. KIM : Specification-based approach of Behavior Control for TOS
- W. SHIN : The Extended Role Based Access Control for Trusted Operating Systems and its Formal Specification
- J. H. CHO : The design of Secure File Systems for Trusted Operating Systems
- T. Tabata: On the Security of Integration of SELinux Access Permissions

[Data mining]
- H. J. YOO : Privacy Preserving Data Mining : Randomization approach
- C. Su: ITR: Distributed Data Mining to Protect Information Privacy Chris Clifton (paper introduction)

[Mobile Agent]
- J. Y. PARK : Agent Key and Secure Computing Base for Mobile Agent Protection
- Y. Kotegawa: End-User Security Management with Mobile Agents

[IDS]
- K. Tatara: A Probabilistic Method for Detecting Anomalous Program Behavior

[Access Control]
- S. Amril: Specification and Validation of Enterprise Access Control Data for Conformance to Model and Policy Constraints (paper introduction)

[E-mail filtering]
- M. Iwanaga: Some adjustment for Bayesian filtering for Japanese environment

研究情報源の収集

- リンク集としてまとめた
  - OSセキュリティの分野ごとに情報収集
    - セキュアOSやOS開発のプロジェクト
    - Sandbox
    - Anomaly Detection based on System call
    - Overflow
    - Embedded system
  - 研究者や研究グループの調査

アンケートの結果（1）

- 本プロジェクトに対するアンケートを企業参加者の方々に実施した
- 参加動機
  - 上司からの勧め（知見を広める意味で参加）
  - 今後はセキュリティへの取り組みが必須と考え，参加
  - 調査研究テーマが研究対象と同じであったため
- 活動に対する満足度
  - 成果面はほぼ満足だが，運営面で不満あり
    - 企業メンバーの役割が不明確
    - 役割分担で大学と企業で意識のずれがあった
  - 打ち合わせでの報告内容は専門性が強すぎた
    - 企業で即製品適用できる技術提案がもっとあればよかった
  - 韓国のセキュアOSの動向，活動などは非常に有意義だった

アンケートの結果（2）

- 改善すべき点
  - 企業側の活動はどうしてもボランティア的活動になってしまうため，企業側の負担が大きい
  - 企業側のメリットが明らかになるとうれしい
    - 企業の持つ技術の標準化・普及，企業間連携など
  - 全般にコミュニケーション不足だった
    - メイリングリストの活用
    - WikiやBlogでサイトを構築すると活発にやり取りできたかもしれない

アンケートの結果（3）

- 今後の活動に対する要望
  - OSを含むプラットフォームセキュリティは必須のため，今後も何らかの形で活動を継続して欲しい
  - 技術動向の調査を行うのみでなく，新技術の試作や評価等にまで踏み込んで欲しい．
  - 産学での研究に対する需要と供給のズレがあると思うが，それを埋める活動になれば良いと思う．そういう意味では今回のテーマは良かった．

産官学project

- SSR project　[産学]
- 21s世紀COE@文科省[官学]

韓国？

韓国の ITRC 紹介
< Information Technology Research Center>

http://forum.itrc.or.kr/forum/Itrc_Info.htm

Sponsor : Ministry of Information and Communication
Rep. of Korea

九州大学

許　容碩

事業概要

事業目標

大学に結集されている人的資源を積極活用して IT核心技術を開発してプロジェクト遂行能力がある高級研究人力を養成するために大学 IT研究センターを集中育成支援

主要事業内容

- **支援対象** : 大学内 IT研究センター
- **支援内容** : 参加研究員人件費, 研究機資材及び研究費支援
- 研究センター当り 8年間毎年平均 8億ウォン程度
  (2002年までは 4年間毎年平均 4億ウォン程度)
- 毎年厳格な評価を経って支援対象調整及び差等支援を通じた競争環境造成

推進実績 (1)

■ 2000年

- 計 25個研究センター選定支援
  (既存指定 16個 + 新規選定 9個)
- 新規指定 9個は 4年間年間 4億ウォン内外の研究費支援
- 既存指定 16個センターは 3年間支援(2000.8 - 2003.7)

■ 2001年

- 新規選定 8個センターを含んで計30個研究センター支援
- 既存指定センターの中で評価によって 3個センター支援中断
- 新規 8個センター追加選定

推進実績 (2)

■ 2002年

- 新規選定 4個センターを含んで計32個研究センター支援
- 既存指定センターの中で評価によって 2個センター支援中断
- 新規 4個センター追加選定

■ 2003年

- 新規選定 11個センターを含んで計39個研究センター支援
- 既存指定センターの中で評価によって 3個センター支援中断
- 新規 11個センター追加選定

区分	2000	2001	2002	2003	2004	計
新規指定 (個)	25	8	4	11		
支援中断 (個)		3	2	4		9
総支援センター (個)	25	30	32	39	46	
支援予想 (億ウォン)	100	130	142	315.6	100	687.6

期待される効果 (1)

- センター当り大学院生を年間 40人以上にすることで主要核心技術分野に修,博士級高級人材を安定的に供給
- 学制間研究を支援することで多様な技術分野の融合が必要な技術開発が可能であり,プロジェクト開発遂行能力がある高級研究人力養成
- 産学研共同研究を勧奨することで開発技術の企業へ移転や商用化, 企業側が解決困難な研究などを促進して産業競争力を向上

期待される効果 (2)

- 国際共同研究を支援することで研究者の国際競争力を向上して, 世界的水準の研究成果導出及び国際標準を先導
- ITRCで輩出された修,博士人力の世界優秀な企業体及び研究所就業を積極支援してシリコーンバレーなど世界の IT 現場でアメリカ, インド, 中国など世界 IT エンジニアたちと競争を促進

※成果物 : 国内.国際特許, SCI 論文, S/W, 研究開発試作品
産学研協力構築実績(件数,金額), 国際共同研究実績(件数, 金額)

センター紹介 (1)

分類	技術分野	研究センター
SW/ デジタル コンテンツ (13),	デジタル コンテンツ (8)	• 知能型GIS研究センター (Inha Univ.) • e-ビジネス技術研究センター (Seoul Nat' l Univ.) • ソフトウェアプロセス改善センター (KAIST) • コンピューターグラフィックス/バーチャルリアリティー 研究センター (Ewha womans Univ.) • マルチメディアコンテンツ研究センター (Dongshin Univ.) • ゲームアニメーションセンター (Ajou Univ.) • Grid ミドルウェア研究センター (ICU) • デジタル製造情報技術 (Ulsan Univ.)
	Embedded SW (2)	• ソフトウェア研究センター (Konkuk Univ.) • 次世代イムベデードソフトウェア開発環境研究センター (Sunmoon Univ.)

センター紹介 (2)

分類	技術分野	研究センター
SW/ デジタル コンテンツ (13),	デジタル TV (3)	・次世代放送技術研究センター (Yonsei Univ.) ・実感放送研究センター (KJIST) ・メディアサービス技術研究センター(Kwangwon Nat'l Univ.)
HW 部品 (13),	知能型サービスロボット(1)	・知能型サービスロボット研究センター (KAIST)
	次世代 PC (4)	・情報通信素材研究センター (Hanyang Univ.) ・次世代 3D ディスプレー研究センター(Kwangwoon Nat'l Univ.) ・プラスチック情報素材研究センター(Pusan Nat'l Univ.) ・IT用エネルギー保存及び変換技術研究センター (Gyeongsang Nat'l Univ.)

センター紹介 (3)

分類	技術分野	研究センター
HW 部品 (13)	IT SoC (4)	・コムピュテイショノルエレクトロニクスセンター(Inha univ.) ・RFICセンター (Kwangwoon univ.) ・高性能集積システム研究センター(KAIST) ・IT SoC 設計技術研究センター (Yonsei Univ.)
	テレメティックス (4)	・電磁波環境技術研究センター (Chungnam Nat'l Univ.) ・次世代 LBS 応用研究センター(Chonbuk Nat'l Univ.) ・Vehicular Infotronics 研究センター (Chonbuk Nat'l Univ.) ・テルレメティックス要素技術 (Cheju Nat'l Univ.)

センター紹介 (4)

分類	技術分野	研究センター
通信/情報保護/その他 (17)	ホームネットワーク (2)	・超広帯域無線通信研究センター (Inha Univ.) ・ホームネットワーク研究センター (Chung-ang Univ.)
	次世代移動通信 (4)	・次世代無線通信研究センター(Seoul Nat'l Univ.) ・モバイルマルチメディア研究センター (ICU) ・ HY-SDR 研究センター (Hanyang Univ.) ・OFDM基盤広帯域センター (POSTECH)
	BcN (4)	・次世代インターネット研究センター (Korea Univ.) ・広帯域移動マルチメディア研究センター (Sungkyunkwan Univ.) ・次世代光-無線加入者網研究センター (KJIST) ・BcN エンジニアリング研究センター (ICU)

センター紹介 (5)

分類	技術分野	研究センター
通信/情報保護/その他 (17)	情報保護 (5)	・情報保護技術研究センター (Korea Univ.) ・情報保護認証技術研究センター (Sungkyunkwan Univ.) ・Linux システム保安研究センター (Chonnam Nat'l Univ.) ・移動ネットワーク情報保護技術研究センター (Kyungpook Nat'l Univ.) ・インターネット侵害対応技術研究センター (Chungnam Nat'l Univ.)
	RFID/USN(1)	・次世代 RFID/USN 研究開発 (Yonsei Univ.)
	その他 (1)	・通信数学センター (Korea Univ.)

センター紹介 (6)

分類	技術分野	研究センター
政策分野 (3)	IT 融合技術政策 (1)	・技術及び革新政策研究センター (ICU)
	通信放送 融合技術政策 (1)	・通信放送融合技術政策研究センター (Seoul Nat'l Univ.)
	次世代 無線通信政策 (1)	・次世代無線通信政策研究センター(Hanyang Univ.)

27大学 46個研究センター

情報保護分野の センター(5個)紹介

情報保護技術研究センター
(Korea Univ.)

■研究期間：2000.7 – 2004.8 (1段階完了:暗号技術分野の最優秀センター選定),
2004. 9 – (2段階)

■センター長: Prof.Jongin Lim (Korea Univ.)

■参加教授 http://cist.korea.ac.kr/new/index.html : only Korean

Korea Univ, (Jongin Lim, Donghoon Lee, Sangjin Lee)
Korea Univ, (Jongsub Moon, Hyungjin Yang, Seokhee Hong)
Korea Univ, (WhiKap Cho, Youngho Park, Seokwon Jung)
Semyung Univ, (Changhan Kim)
Baejae Univ, (Suhak Sung)
Kookmin Univ, (Okyeon Lee)
Safedigm Inc.(Changhee Lee)
BCQRE Inc.(Sungjun Park)

情報保護認証技術研究センター
(Sungkyunkwan Univ.)

■研究期間：2000.7 – 2004.8(1段階完了), 2004. 9 – (2段階)

■センター長: Prof.Dongho Won (Sunkyunkwan Univ.)

■ 2段階の組織 http://dosan.skku.ac.kr/~atrc/index.html : only Korean

次世代超軽量 / 低費用認証源泉技術開発	Sungkyunkwan Univ, (Dongho Won)
	Sungkyunkwan Univ, (Daeho Jo)
USN 環境に相応しい AAA 技術開発	Sungkyunkwan Univ, (Taemyung Jung)
	Ewha womans Univ, (Gi-Jun Chae)
	Hongik Univ, (Youngcheol Shim)
情報家電ネットワークでの認証技術開発	Yonsei Univ. (Jusuk Song)
	Sungkyunkwan Univ. (Hyungseng Chu)
	Sejong Univ. (Taekyung Kwon)
データ接近制御及び侵入感耐技術開発	Sungkyunkwan Univ. (Seongju Kim)
	Sungkyunkwan Univ. (Ungmo Kang)

Linux システム保安研究センター
(Chonnam Nat'l Univ.)

■研究期間：2000.8 – 2008.7
■センター長: Prof.Bongnam Noh (Chonnam Nat'l Univ.)

■ 組織 http://lsrc.chonnam.ac.kr/ : only Korean

侵入対応技術開発	Chonnam Nat'l Univ, (Bongnam Noh)
	Soongsil Univ, (Youngsung Moon)
	Chonbuk Nat'l Univ, (Moonho Lee)
侵入感耐技術開発	Sungkyunkwan Univ, (Youngik Um)
	Hannam Univ, (Jaekwang Lee)
	Inchon Univ, (Byungjun Min)
保安管理技術開発	Wonkwang Univ. (Hyunghye Lee)
	POSTECH (Jong Kim)
侵入パターン及び検証技術開発	Yonsei Univ. (Sungbae Joo)
	Mokpo Uinv. (Jaehyeon Seo)

協力企業 / 機関
韓国電子通信研究院
韓国情報保護振興院
(株)Secuve
(株) igloo sec.
(株) Inzen

No.55

移動ネットワーク情報保護技術研究センター
(Kyungbuk Nat'l Univ.)

■研究期間：2000.6 –
■センター長: SangJae Moon (Kyungpook Nat'l Univ.)

■ 組織 http://msrc.knu.ac.kr/eng/introduction1.htm : only English

Interface Information Security Technology	Kyungpook Nat'l Univ, (Sang-jae Moon)
Core RadioNetwork Security Technology	POSTECH (PilJoong Lee)
Home network Security Technology	Kyungpook Nat'l Univ. (Sangwook Kim)
Security Evaluation Mobile Network SecurityTechnology	Pukyung Nat'l Univ. (Jihwan Park)

協力企業 / 機関
Dittotechnology Inc.
CompuKorea
Modennet
Hyundaist
Shinwontechnology

No.56

インターネット侵害対応技術研究センター
(Chungnam Nat'l Univ.)

■研究期間：2003. 7 –
■センター長: Jae-cheol Ryou　(Chungnam Nat'l Univ.)

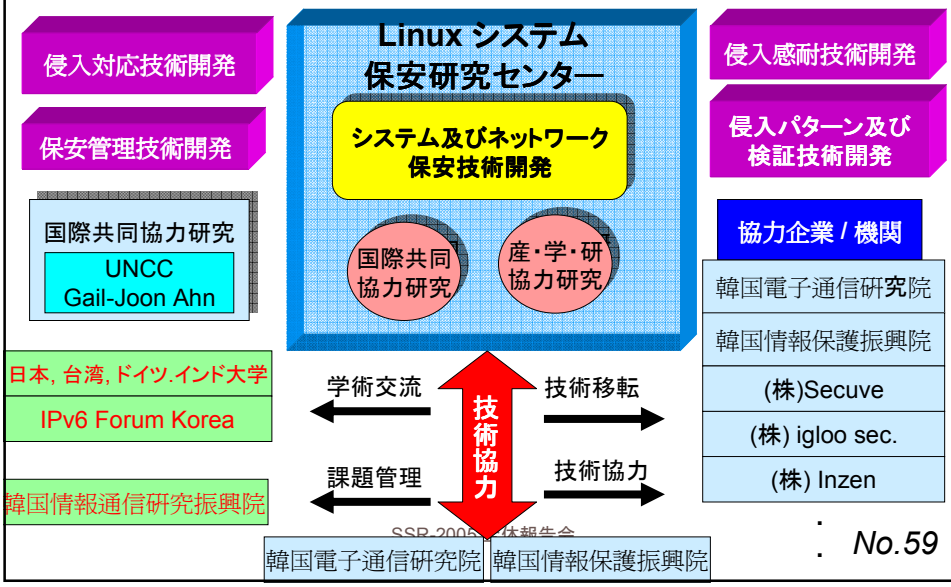
■ 組織 http://iirtrc.cnu.ac.kr/intro.html : only Korean

Intrusion Detection . Protection Research Team	Network Intrusion Detection Response Research Team	Integrated Security Technology Research Team	Internet Intrusion Response lab

Chungnam Nat'l Univ. (Jae-cheol Ryou, Taeck-geun Kwon, Hyong-Shik Kim)
KAIST (Sehun Kim, Sung-Deok Cha)
Soonchunyang Univ. (Heung-Youl Youm)
Hanshin Univ. (Hyung-woo Lee)
Hanyang Univ. (Jae-il Jung)
Kyunghee Univ. (Choong-seon Hong)

Linux システム保安研究センター
(Chonnam Nat'l Univ.)

構成



No.59

産・学協同モデル(1)

- 産学協力Workshop開催 (2回/年間)
  - 産業体から技術を検証受けて, 要求事項を反映する.
  - 保安産業体の要求事項取り集めて研究に反映する.
  - 研究された主要技術を説明して関心を表明する産業体に技術移転協約を締結する.
- 産業体専門家の中間評価後研究教授たちの開発戦略点検 (2004年 2月)
  - 研究開発内容に対する開発戦略を点検する.
  - 研究開発技術及び予想結果物に対する産業体に広報と技術移転を促進及び誘導する.

産・学協同モデル(2)

■ 産学共同研究協約締結

- ITRC Forumを通じて主要開発技術に対する協約を締結を誘導する.
- 産業体を訪問して本センターの開発技術に対して広報して共同研究を誘導する.
- 既存に産学協力協約を締結した業体に主要技術に対する技術移転協約を誘導する. : ㈱Secuve ㈱Inzen ㈱igloo sec. など

■ 国内情報保護関連研究所の技術自問

- 韓国情報保護振興院, 韓国電子通信研究院などの国内情報保護関連研究所に 産業化の妥当性, 世界的な技術水準に対する比較, 技術開発方向点検などを自問受ける.

研究課題管理

○12個参加大学の共同研究推進

- 全南大Linuxシステム保安研究センター(LSRC, Linux Security
- Research Center)を中心に 4個詳細課題に 12個参加大学が課題を共同で推進

○定期的な研究結果発表会開催 (6回/ 年)

- 3次年度まで 6回/年の定期的な研究結果の点検のため会議進行
- 参加教授間の技術交流及び研究方向の点検

○研究計画に対する実績と研究貢献度による研究費分配

- 研究実績の評価指標を自主的に作成して事前公知
- 2004年 1月 : 外部専門家による研究内容中間評価施行
- 2004年 5月 : 外部専門家に依頼して研究遂行に対する総合評価施行
- 研究計画に対する実績に対する評価と中間評価, 総合評価に基礎で次年度の研究費を差等支給
-中間評価及び課題参加度によってインセンティブ(Incentive)支給

韓国でのTrusted OSの研究開発(1)

- 韓国のTrusted OSの研究開発は1990年代半ばから始まった
  - 最初の研究はアクセス制御やTrusted OSのサーベイ
- KISAやETRIの研究者が先駆者となった
  - 数個のプロジェクトを遂行
- 韓国で最初の商用バージョンの公表は2000年
  - TSonNet, Secuve
  - 最近では10程度の会社がKISAからのCC (Common Criteria)の評価を待っている
  - ETRIは研究を現在も続けており，FreeBSDをベースとしたTCSEC B2相当のTrusted OSを開発している
  - KISAは他の商用セキュリティ製品と同様にTrusted OSを評価する立場にある

韓国でのTrusted OSの研究開発(2)

- 韓国で開発されたよく知られたTrusted OS
  - L4Linux-MLS and RedOwl SecuOS
  - SecuROS
  - SecuveTOS
  - SeeCure OS
  - 他に11程度のTrusted OSがある
- 大学においても1990年からOSセキュリティに関する韓国の国内会議で成果が発表されている
- 研究開発の動向は，世界的な動向を追っている
  - MACやRBACの実装
  - 強制機構とポリシ機構の分離
  - モジュールとしての実装

組み込みシステムのセキュリティ

- 背景
  - 適用拡大とリスク増大
    - 自動車，携帯電話，家電など
    - 病院や高圧送電システムなどの重要な施設や機器の誤動作が危険を伴う場合，リスクが大きい
- 課題
  - 処理能力
  - バッテリ
  - 柔軟性
  - 破壊改ざんからの保護
  - コスト
  - 相互作用

組み込みシステムセキュリティの動向調査

- 調査文献
  - P. Koopman, “Embedded System Security,” IEEE Computer, Vol.37, No.7, pp.95-97 (2004).
  - S.Ravi, et al, “Security in Embedded Systems: Design Challenges,” ACM Transaction on Embedded Computing Systems, Vol.3, No.3, pp.461-491 (2004).
  - P. Kocher, R. Lee, G. McGraw, A Rachunathan, S. Ravi, “Security as a New Dimension in Embedded System Design,” Proceedings of DAC 2004, ACM IEEE. Pp.753-760 (2004).
- 文献調査の結果やWeb上の最新動向をまとめ，調査結果をWebに掲載

OSのセキュリティの必要性

- 従来のOSの問題点
  - パーソナルコンピュータ
    - ウイルス、スパイウェア、キーロガー…
  - サーバのOS
    - デーモン(WWW, FTP, Sendmail), DoS …
  - セキュリティパッチにより脆弱性を取り除く
    - ゼロディレイアッタク

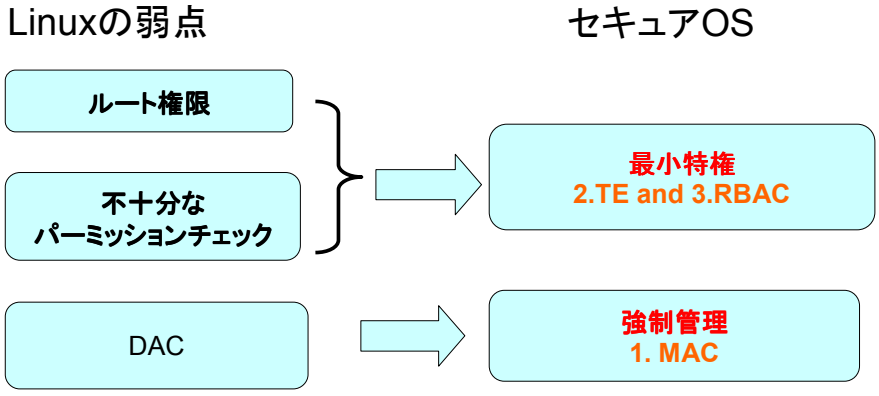
      ⇒十分な方法とはいえない

（PPT edited by 長野 文昭）

セキュアOSのコンセプト

- セキュアOSのコンセプト
  - MAC
    - Mandatory Access Control
  - TE
    - Type Enforcement
  - RBAC
    - **Role-Based Access Control**

セキュアOSのコンセプト



1. MAC

Mandatory Access Control

- 通常のLinux: Discretionary Access Control (DAC)
- DAC: オブジェクトの所有者がアクセス権限を決定
- MAC: 管理者がオブジェクトのアクセス権限を決定

⇒全てのアクセス権限は管理者により決定される

管理者による管理が容易

2. TE

Type Enforcement

- type/domainを定義する
  - typeはオブジェクト、domainはプロセスにつけられる
- domainがtypeにどのような操作を実行できるかを決定

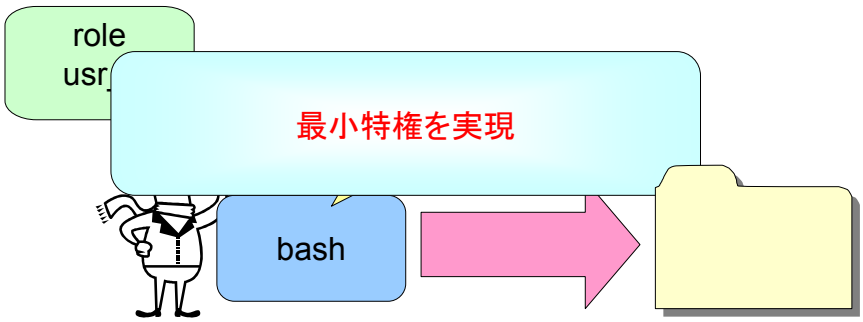
例：

3. RBAC

Role-Based Access Control

- ユーザの役割ごとに、利用できるdomainを設定

例：



OSセキュリティの調査(I)

- Trusted OS Research and Development[1]
  - Including Korean cases -
  Hyung Chan Kim, Wook Shin, R. S. Ramakrishna

Commercial products of Trusted OS
(except Secuve and TSonNet)

OSセキュリティの調査結果(II) by 鑪

- バッファオーバフローを利用する侵入行為への対策技術
  - 攻撃者はプログラムに内在するバグを利用して任意のコードを実行するという仮定
- プログラマ側の対策技術
  - パターンマッチング技術
  - 構文解析技術
  - コンパイル時にセキュアなコードを生成する技術

OSセキュリティの調査結果

- ユーザ（管理者）側の対策技術
  - メモリ管理機構を用いる対策技術
  - Sandboxを用いた対策技術
  - MAC (Mandatory Access Control)
  - RBAC (Role Based Access Control)
  - MLS (Multi Level Security)
  - TE（Type Enforcement）
  - システムコールを用いる異常検知
  - バイナリコードを解析する技術
  - ライブラリに基づく技術

パターンマッチング技術

- ソースコードに脆弱性のある関数が含まれるかどうかを走査
  - 発見時には検知結果を目に見える形で表現
  - ITS4，RATS, Flawfinder等が存在
  - パターンマッチングによって発見された脆弱性の情報を基に、ソースコードをセキュアなものに置き換える研究なども行われている(Haugh et al. ‘03)
  - 利用者が独自定義した関数は検出の対象外

構文解析技術

- 構文解析を用いてソースコードを抽象化した構文木に変換
  - ソースコード内部の論理的な矛盾点を発見することを目的
  - Splint(LCLint)、Cqual
  - 構文解析に制約を加えることによってバッファオーバフロー脆弱性の検出精度を上げる研究(Larochelle et al. ’01)
  - 論理的な構造を解釈するためにソースコードに対して解析ルールとして注釈を記述する必要
  - ソースコードの静的解析技術を異常検知に適用した研究(Wagner et al. ’01, Oyama et al. ’03)

コンパイル時にセキュアなコードを生成する技術

- 潜在的にバッファオーバフロー脆弱性を内包するソースコードから安全な実行コードを生成
  - StackGuard、Stack Smashing Protector(SSP)、Bounds Checking、PointGuard
    - StackGuardとSSPはリターンアドレスの前にカナリアと呼ばれる値を挿入して書き換えられているかをチェック
    - SSPやPointGuardには内部で用いられている変数や引数の保護により、関数ポインタを持つ変数を狙った攻撃に対する防御
    - Bounds Checkingは変数や配列の生成、利用、削除を追跡

メモリ管理機構を用いる対策技術

- OSの機能を拡張することによってプログラムを安全に実行する環境を整える技術
  - Openwallはユーザメモリ領域においてスタック内の実行コードを実行できないようにする機能を持つ
- スタックの非実行化機能では検出できないバッファオーバフロー攻撃というものも存在(ヒープオーバフロー)
- 次のような手段で侵入を果たすことも可能 (Linus Torvalds, '98)
  1. バッファオーバフローを起こしてリターンアドレスをsystemライブラリ関数へのポインタで書き換える
  2. スタック上の次の4バイトは無意味なものでよい(system関数のリターンアドレス)
  3. 次の4バイトは共有ライブラリ上の/bin/sh文字列が記述された位置へのポインタで書き換える(system関数の引数)と、system関数は引数として渡された文字列を/bin/sh -cの引数にして実行
- OpenBSDでは、プログラムを実行時にスタック領域やヒープ領域のアドレスを確率的に決定する試み

Sandboxを用いた対策技術

- ファイルシステムを拡張することによりアプリケーションプログラムから識別可能なディレクトリ構造を制限
  - 被害を最小限に抑制
- Janus 、Mapbox、SBOX、Consh
  - ユーザレベルにおいてシステムコールの発行するプロセスを補足
- SubDomain、TRON、DTEなど
  - カーネル内にリファレンスモニタを実装した研究
- Javaのようにプログラミング言語レベルでの実装

MAC(Mandatory Access Control)

- システムにより決められたポリシに基づいたアクセス制御が強制
  - システムで決められたポリシに基づく制御の判断をするための属性が付加
  - 機密度を表すタグはラベルと呼ばれ，MLS（マルチレベルセキュリティ）の要
  - 近年多くのセキュアOSに実装（Trusted Solaris、SELinux）

RBAC (Role Based Access Control)

- RBACでは管理作業を担うユーザに制限付きの管理権限を割り当てることを可能
  - 一連の管理作業を果たすための必要最小限の権限を付与
  - 管理者に必要以上の権限を与えず危機の最小化と複数のユーザによる管理の分散を実現
  - RBACの実装例にはSolaris8，9，SELinuxなどが存在

MLS (Multi Level Security)

- MAC を実現するサブジェクト（ユーザやプロセスなど）とオブジェクト（ファイル、ディレクトリなど）とに分類
  - サブジェクトには機密ラベルと権限が付与
  - オブジェクトに対するアクセスでは、オブジェクトに付与された機密ラベルルとの優位性により判定
- 与えられた権限よりも高い機密区分の情報にアクセスするのを阻止
- MLSの実装例としてTrusted SolarisやSELinuxがある

TE（Type Enforcement）

- サブジェクトとオブジェクトとの間の関係でアクセスを制御する機構
  - システム上に存在し得るすべてのサブジェクトとオブジェクトにはアクセス制御のためのラベルが付与
  - TE ではサブジェクトとオブジェクトに付与されたアクセス制御方針によってシステムレベルでその制御方針を強制的に執行

システムコールを用いる異常検知

- プログラムが発行するシステムコールシーケンスをN-gramと呼ばれるサブシーケンスに分けて正常動作を特徴付けることを提案(Forrest et al. ’96, ’98)
  - N-gram手法に関連する研究としては、システムコールシーケンスから得たN-gramに対してデータマイニングを適用(Lee et al. ’98)
  - N-gramにおけるNの長さを可変にする研究(Marceau et al. ’00)
  - N-gramにおける個々のシステムコール間の発行時間間隔に着目した研究 (Li ’01)

システムコールを用いる異常検知

- システムコールの発行を状態遷移と捕らえるFinite State Machineに基づく手法(Sekar et al. 01’)
  - Kosoresowらはシステムコールシーケンスの中に周期的に見られるサブシーケンスをそれぞれ状態として定義(Kosoresow et al. ’97)
  - Hidden Malkov Model（HMM）を用いたモデル化を行う手法(Warrender et al. ’99)
- システムコールの引数についてモデル化を行った研究(Kruegel et al. ’03)
- システムコールに基づいたエージェントベースの学習システム(Helmer et al. ‘42)
- ソースコードの静的解析技術を利用する研究
  - 状態遷移を非決定的に把握するプッシュダウンオートマトン（NDPDA）を生成(Wagner et al. ’01)
  - スタック情報を利用して制御フローを決定的に把握(Oyama et al. ’03)

バイナリコードを解析する技術

- ソースコードをコンパイルすることで得られるバイナリコードに対して、解析や修正を行う技術
  - バイナリコードの静的解析と書き換えを提案(Prasad et al. '03)
  - サーバに送られてくるバイト列に著しい実行可能命令列が観測された場合に侵入行為と判定(Toth et al. '02)
  - バイナリコードを解析する技術はアプリケーションの再コンパイルが必要ないなどの利点

ライブラリに基づく技術

- ライブラリ技術ではアプリケーションプログラムが利用する脆弱性を含むライブラリを修正することでセキュリティを向上
  - Libsafeやlibparanoiaのようなものがⅰ存在
  - 置き換えられた関数を利用した攻撃しか検知できないという欠点
- ライブラリコールを用いる異常検知の研究も行われている

セキュアOS関連の研究動向

- IPAによるアクセス制御関連の調査
  - 16年度事業として以下の3テーマを実施
    - アクセス制御に関するセキュリティポリシーモデルの調査
    - 電子政府システムにおけるアクセス制御要件に関する調査
    - 強制的アクセス制御に基づくWebサーバに関する調査・設計
  - 電子政府におけるセキュリティに配慮したOSを活用した情報システム等に関する調査研究
    - セキュアOSの概説
    - 認証システム，文書管理システムへのセキュアOSの適用可能性について検討
    - 報告書は今月中に公開予定

セキュアOS関連の研究動向（2）

- 産業界でも，セキュアOSの技術への関心やニーズの高まり
  - しかし，セキュアOSの本格的な採用や事業化はこれから
- 大学においても，セキュリティに関する研究への関心は高い
  - 近年のセキュリティ関係のシンポジウムの発表件数と参加者の増加
  - 日本は韓国に比べて，システムセキュリティの研究者が少ない

産官学

- 日本

産官学

大企業の研究所

NICT, Security@産総研

- 韓国

産官学

ETRI NSRI, KISA

三星

今後（計画）

- 研究班の継続（GIST, 企業）
  - Mr. HC KIMの博士取得までは
- アジアとの連携（韓国）
  - 中国、シンガポール、インド
- OS セキュリティ ➔ 計算機システムセキュリティ
  - Database security (価格.com事件)

まとめ

- 韓国の研究者と連携し，OSのセキュリティ技術と韓国でのセキュアOSの研究状況について調査
- 韓国の研究プロジェクトについても調査
- 韓国の研究者と共同研究成果も発表

- 本プロジェクトでは，運営面で反省する面があったものの，OSを含めたプラットフォームセキュリティの研究は今後も必要と考えられ，このような産学の連携をより発展させる必要がある．

賛助企業・SSR事務局・関係の諸先生方

助成いただき本当に
ありがとうございました。

付録

共同研究の発表文献

- CSS（コンピュータセキュリティシンポジウム）2004
  - Hyung Chan Kim, R. S. Ramakrishna, Kouichi Sakurai, "On the Privilege Transitional Attack in Secure Operating Systems", Computer Security Symposium 2004(CSS2004), pp. 559-564, Oct. 2004.
  - Ji-Ho Cho, Dong-Hoon Yoo, Hyung-Chan Kim, R. S. Ramakrishna, Kouichi Sakurai, "The Design of Convenient File Protection based on EXT3 File System", Computer Security Symposium 2004(CSS2004), pp. 565-570, Oct. 2004.
  - Wook Shin, Hong Kook Kim, Kouichi Sakurai, "An Implementation of Extended-Role Based Access Control on an Embedded system", Computer Security Symposium 2004(CSS2004), pp. 667-671, Oct. 2004.
- SCIS（暗号と情報セキュリティシンポジウム）2005
  - Hyung Chan Kim, Wook Shin, R.S. Ramakrishna, Kouichi Sakurai, “Constraction of RBAC-Enforceable Secuirty Automata,” SCIS2005.
  - Ji-Ho Cho, Dong-Hoon Yoo, Hyung-Chan Kim, R.S. Ramakrishna, Kouichi Sakurai, “XExt3: The Design and Implementation of a Security Enhanced Ext3 File System,” SCIS2005.

研究費の支出内容

- 共同研究者の旅費と会議参加費（103万円）
  - 国内会議参加と研究打ち合わせのため
- 国内会議の旅費と参加費（49万円）
- 会議費（21万円）
  - 打ち合わせの会議費用
- 雑費（27万円）
  - HP作成などのアルバイト代など