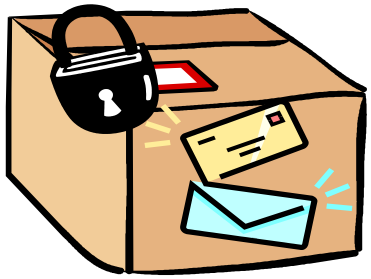
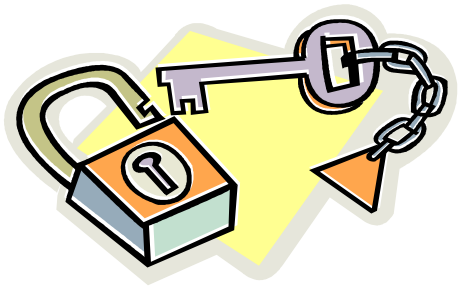
Information Security and Digital Forensics

Drs KP Chow, Lucas Hui, SM Yiu
Center for Information Security & Cryptography (CISC)
邹锦沛，许志光，姚兆明
香港大学资讯保安及密码学研究中心

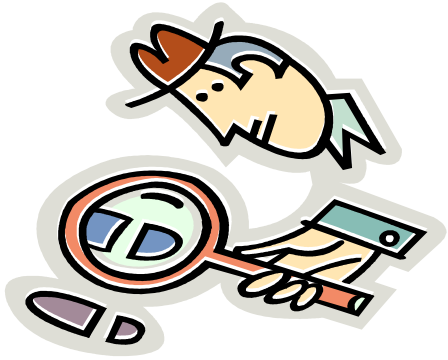
Research Projects in CISC
研究项目

Security and cryptography research





Computer Forensics research



Applications & implementation 应用与实现

Hybrid (software + hardware token, Mobiles) 混合系统 (软件+硬件密钥, 手机)

GPU (图形处理单元卡)

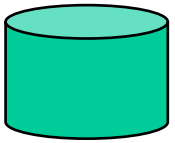
.....

Cryptographic protocol (密码协议)

VANETs (Vehicular ad hoc network) 车辆随意网路

Smart (power) grid system 智能电网系统

Database system 数据库系统 (e.g. data mining with privacy 数据挖掘隐私问题)



Anonymous authentication (credential) in discussion group 讨论组匿名身份验证 (凭据)

.....

Cryptographic primitives 加密基元

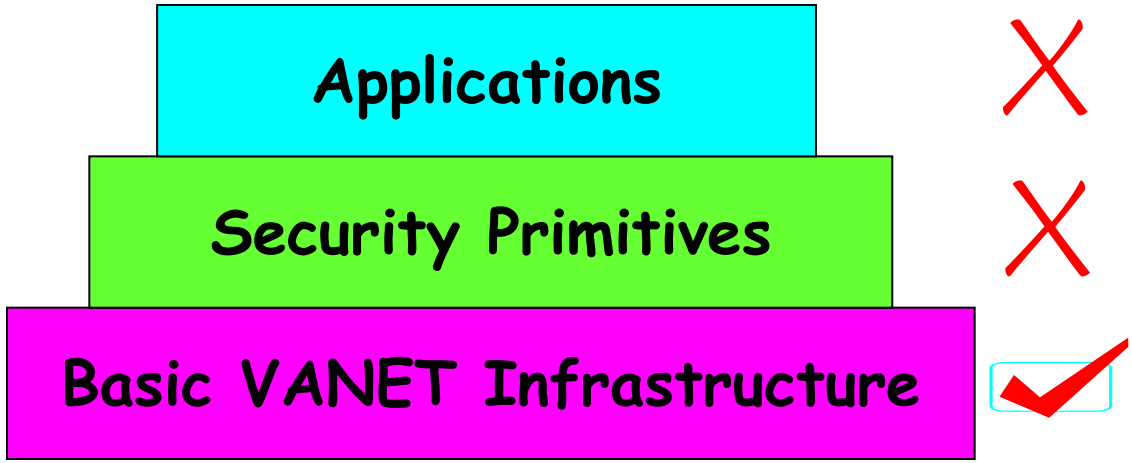
Signature schemes 签名方案

Leakage resilience 泄漏的韧性

.....

Models: Identity-based; PKI-based; Post-quantum
不同的模型: 基于身份, 后的量子密码系统

Our results (我们的研究结果) [2009 -]:



Primitives

- Ad hoc communications
  Authentication of messages from unknown vehicles.
- Group communications
  Authentication of messages from friends
- Multiple level authentication
  Differentiating regular and urgent messages

Applications

- Secure and privacy preserving querying schemes
  OT-based private querying (queries not linked to identity)
  VANET-based navigation (destination not linked to identity)
- Secure taxi service
  Protect safety of taxi drivers and passengers

Selected publications

T.W. Chim, S.M. Yiu, C.K. Hui and V.O.K. Li, "Security and Privacy Issues for Inter-vehicle Communications in VANETs," (SECON'09), June 2009.

T.W. Chim, S.M. Yiu, C.K. Hui, Z.L. Jiang and V.O.K. Li, "SPECS: Secure and Privacy Enhancing Communications Schemes for VANETs," (ADHOCNETS'09), Sep 2009.

T.W. Chim, S.M. Yiu, C.K. Hui and V.O.K. Li, "MLAS: Multiple Level Authentication Scheme for VANETs, Ad Hoc Networks, 10(7), 2012.

T.W. Chim, S.M. Yiu, C.K. Hui and V.O.K. Li, "SPECS: Secure and Privacy Enhancing Communications Schemes for VANETs," Ad Hoc Networks, 9(2), 2010.

T.W. Chim, S. M. Yiu, C. K. Hui and Victor O. K. Li, "OPQ: OT-based Private Querying in VANETs," to appear in the IEEE TITS, 2011.

T.W. Chim, S.M. Yiu, C.K. Hui and V.O.K. Li, "Grouping-enabled and Privacy-enhancing Communications Schemes for VANETs," Invited book chapter, 2010.

T.W. Chim, S. M. Yiu, C. K. Hui and Victor O. K. Li, "VSPN: VANET-based Secure and Privacy-preserving Navigation," IEEE TC, 2012.

Changhui Hu, T.W. Chim, S.M. Yiu, C.K. Hui, Victor O.K. Li, "Efficient HMAC-based Secure Communication for VANETs, Computer Networks, 56(9), 2012.

International Conferences hosted by CISC

- *2007 High Technology Crime Investigation Association (HTCIA) ASIA PACIFIC TRAINING CONFERENCE*. Dec 2007.
- *The 7th International Conference on CRYPTOLOGY AND NETWORK SECURITY (CANS 2008), Hong Kong, Dec 2008.*
- *Sixth Annual IFIP WG 11.9 International Conference on Digital Forensics*, Hong Kong, 2010.
- *Sixth ACM Symposium on Information, Computer & Communication Security (ASIACCS 2011)*, Hong Kong, Mar 2011.
- *Fourteenth International Conference on Information and Communications Security (ICICS 2012)*, Hong Kong, 2012.

Graduates

- Teaching in Universities in HK
- Teaching in Universities in PRC
- Post-doc in USA, HK
- Researcher in research institutes in HK
- Others working in commercial companies in HK, PRC, Singapore, USA (mainly MPhil graduates)

Computer Forensics Research Group
计算机取证
Leader: Dr KP Chow

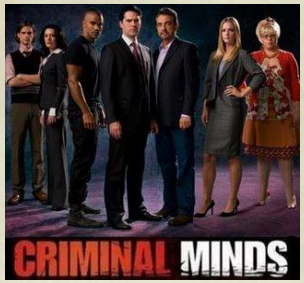
- 一些项目
  - 数字调查和取证:
    - DESK（数字证据搜索工具）
    - BTM（也称为网线监察系统）
    - 拍卖现场监测
    - 互联网监控平台
- 我们的研究
  - 數碼特徵
    - Behavior profiling: 互联网上罪犯的數碼特征
    - Visual profiling: 數碼视觉特征
  - Cybercrime model

我们的研究 – 數碼特征

- 互联网罪犯的數碼特征 (digital identity profiling)
  - 行为特徵 (Behavior profiling)
    - 互联网上侵权罪犯的數碼特征
    - 互联网拍卖欺诈的數碼特征

DIGITAL IDENTIFY PROFILING

罪犯特征 (Profiling)



- 在北美经常使用(e.g. FBI)，主要目的是协助**同系列犯罪的调查**，例如：性侵犯，凶杀，色情凶杀案

- 寻找识别模式（patterns）
- 不是单独依靠罪特征就可以破案

「黎家盈」的博士论文：“互联网侵权的特征”

系到同一嫌疑人

- **网络犯罪有系列本质**（serial in nature）:
  - 网络犯罪的系列本质允许罪犯行为的识别和常量分类（repeating in nature重複性質）

网上用户特性

- 网上用户之间有社会关系
- 网络身份与用户真实身份没有联系
- **在互联网中可以非常容易的隐藏个人真实身份和行为**
- 很多情况下，一个人拥有多个用户帐户
- **判别一系列网络行为是否由一个用户引起还是多个用户涉及是很复杂的**

用户数码特征分析

根據每個用戶的張貼，計算一個**特徵詞的權重向量（a vector of the weights of feature words）**

Computing the weight of a feature word (t) w.r.f. a user (u)? TF-IDF weight (Salton et al.)

$$W(t,u) = TF(t,u) \times \log \frac{|U|}{|\{u' \in U | t \in u'\}|}$$

Total number of users

Frequency of t in u's postings

# of users having t in his postings

Fewer users have the word, the weight larger

A Profile (用户数码特征)

- User dow_jones in uwants.com

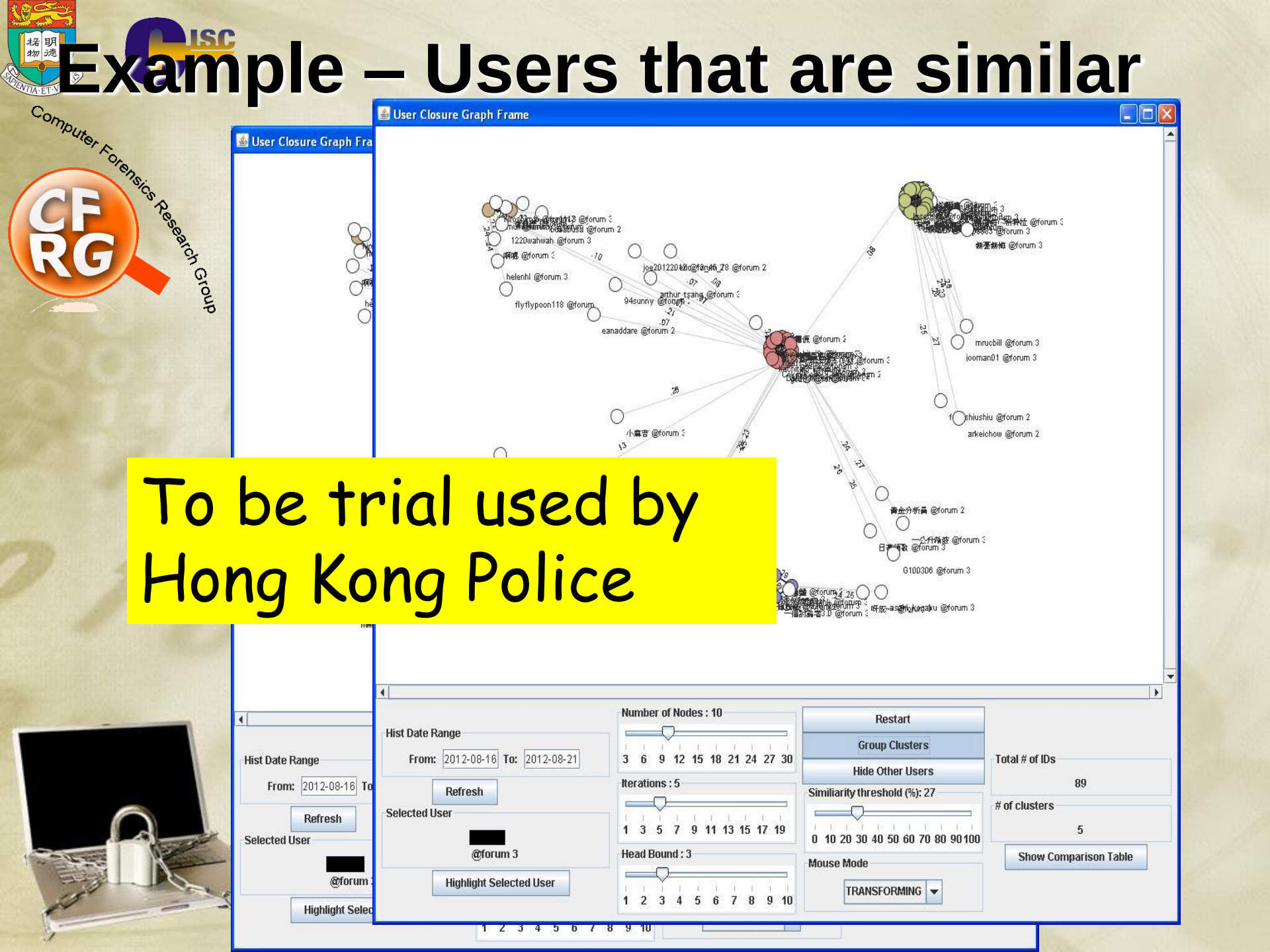
	Feature word	Weight
1	80后	0.21761
2	社民连	0.14349
3	五区	0.12547
4	泛民	0.11357
5	西九	0.10983
6	黄毓民	0.08671
7	功能组别	0.08433
8	总辞	0.08296
9	八十后	0.08194
10	社民	0.08126

使用用户数码特征進行預測

- 這些 discuss.com.hk 論壇上的張貼, 是不是 uwants.com 用戶 dow_jones 發布

Example – Users that are similar

Computer Forensics Research Group



To be trial used by Hong Kong Police

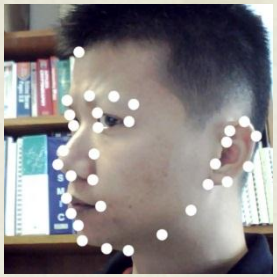
Applications

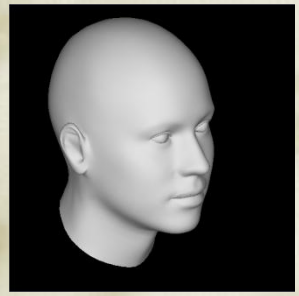
- Trace “real user” behind multiple user IDs
- Track user behavior
- Identify and trace user group
- Predict user and user group behavior
- …

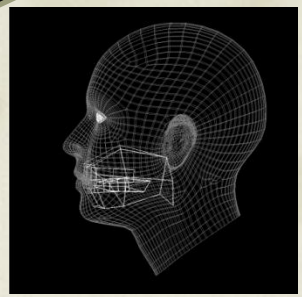
Computer Forensics Research Group

DIGITAL VISUAL PROFILING

人脸重建过程

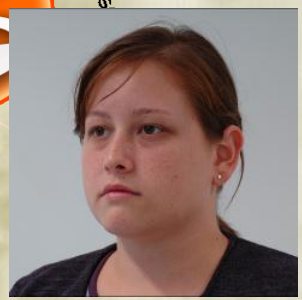


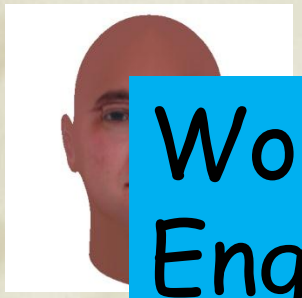
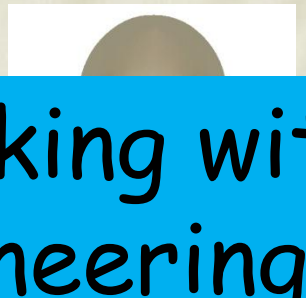


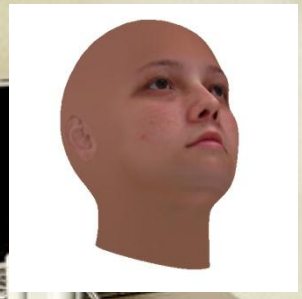


- Facial Feature Detection
- 3D Modeling
- Pose Estimation
- Texture Map Rebuilding

Examples





Working with Wuhan Engineering Science Research Institute for commercialization

Computer Forensics Research Group

CF RG

CYBERCRIME MODELS

贝叶斯网络犯罪模式 (Bayesian Network Crime Model)

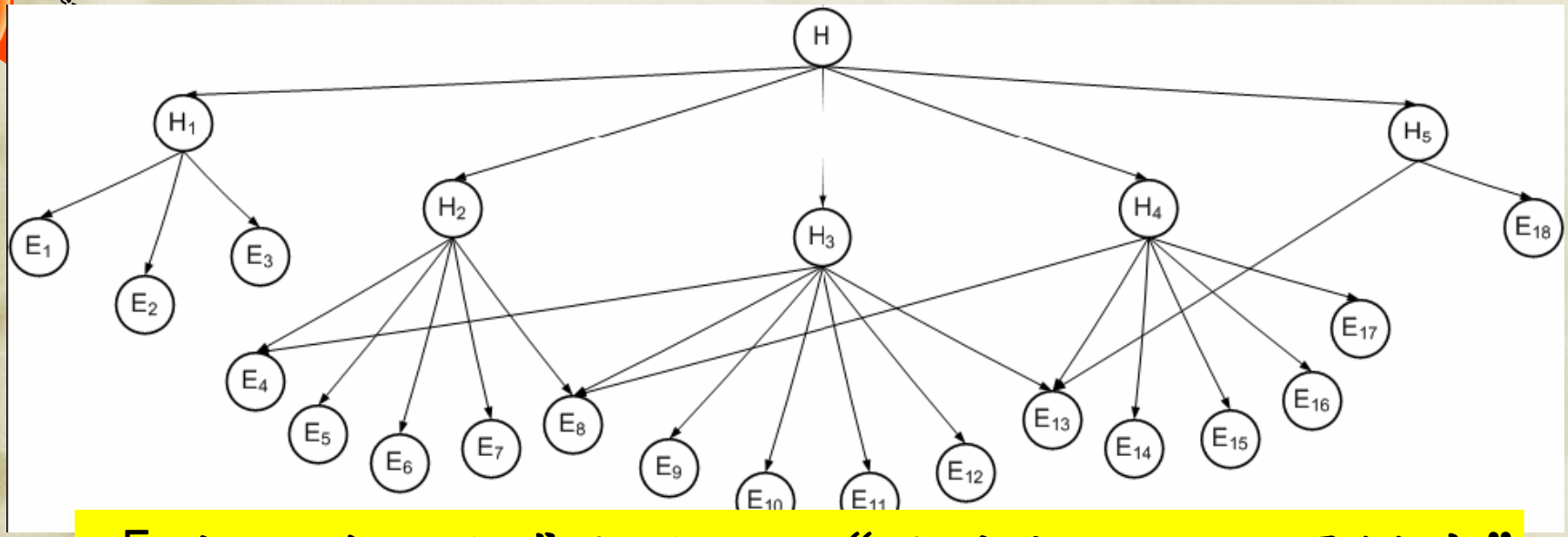
5种贝叶斯网络犯罪模式的定义

- 使用 BitTorrent 分享非法/侵权档案
- 网上拍卖欺诈
- 网上游戏武器被盗
- DDoS 攻击
- 利用数码柜 (Cyber-locker) 分发非法/侵权档案

案例

- A person was arrested by law enforcement officer because he was sharing a movies using BitTorrent
- His computers were seized
- All network access logs were seized
- Is there sufficient evidence to establish his “crime act”:
  - Sharing of copyright protected material
  - Beyond reasonable doubt

BT案例中数字证据的图形表示 (The Big Crook Case)



「关煜群」的博士论文:“贝叶斯网络犯罪模式”

基于案例报道的数字证据，计算H有效的概率是

92.27%

- 于是,法官推断假设H是有效的是否超出合理的怀疑
- 当然，还有其他的案件物证

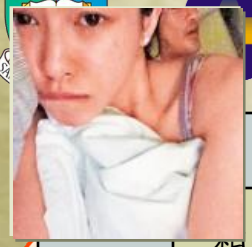
时间的规则 (Time Model)

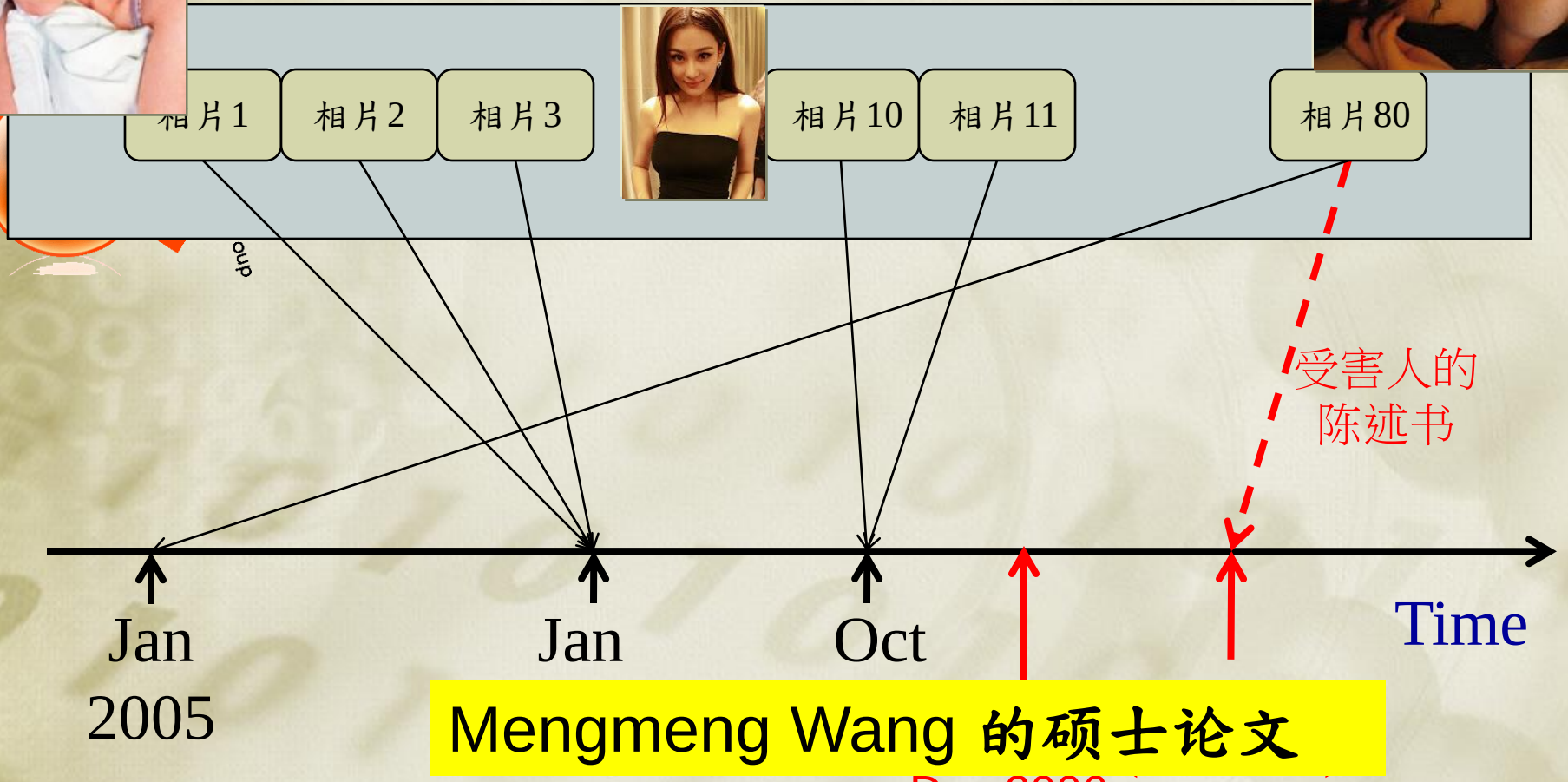
- 支持犯罪事件的重现
- 侧重于NTFS的文件系统的时间分析，并寻求更多有关数字文件的行为特征规则
  - NTFS中采用启发式规则分析MAC时间
- 例如规则 4:
  - 在硬盘驱动器中， 当大量的文件的时间非常接近于*A*时间，文件很可能是由一些扫描工具修改，如反病

Kenneth Tse 的硕士论文

- http://i.cs.hku [illegible] pdf (in Proceedings of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering SADFE 2007)
- **研究论文已数次提交香港法庭**

數碼相機 SD 卡案例





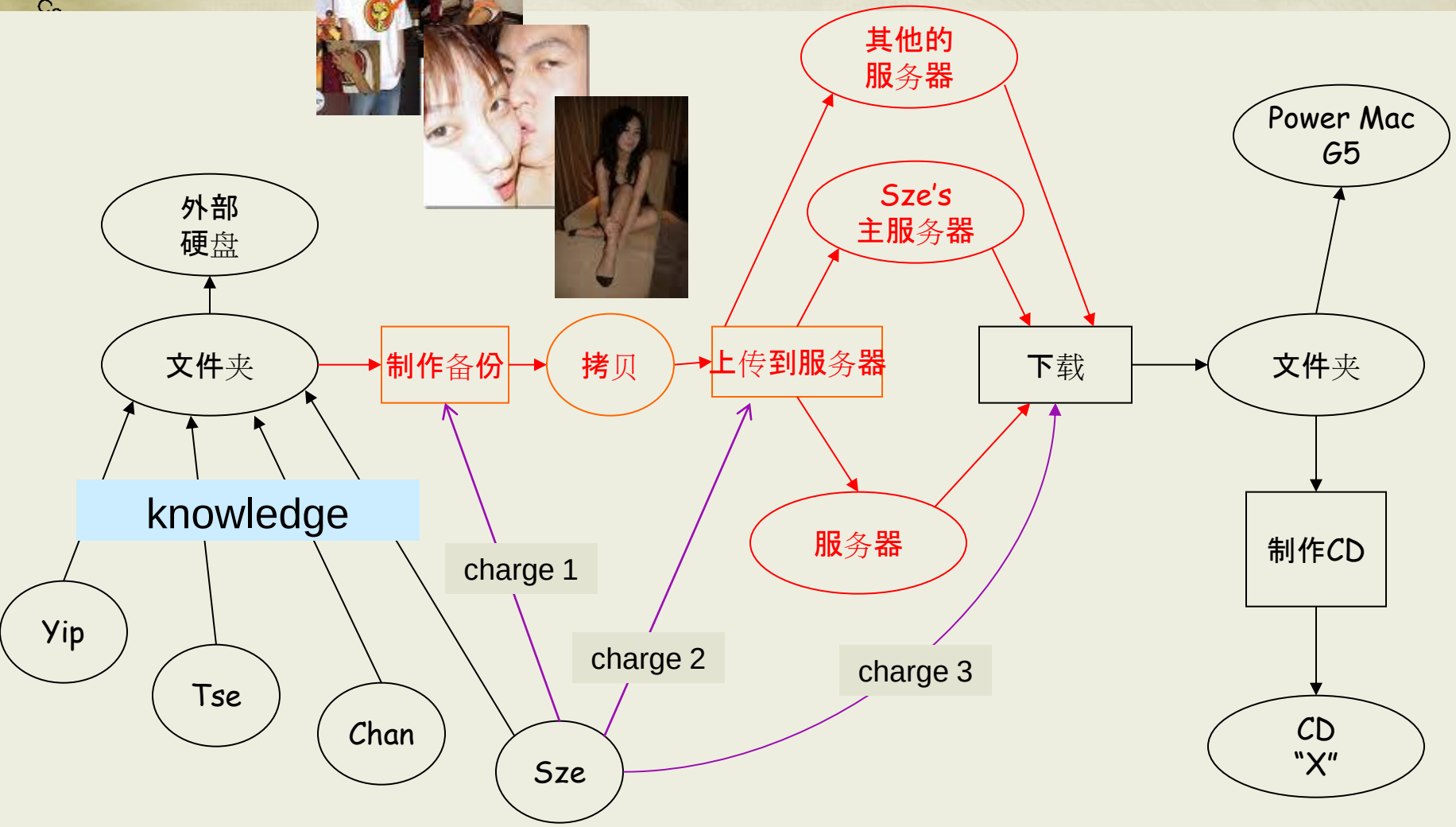
受害人說謊？？
或是創建日期不正確 !!

现场重现 – 陈冠希案例

- 其他人?

- 他是谁?

犯罪现场重现



3种有犯罪或不诚实意图使用电脑:

- 数字证据
- 证人证词
- 数字犯罪现场重现

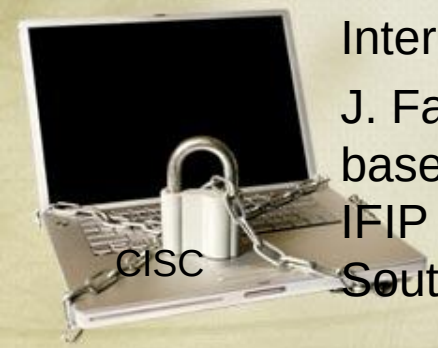
Can we use Bayesian Network to construct the crime scene?

研究者:「谢家树」- 博士研究生

计算机取证 – 中港合作

Computer Forensics Research Group

- **联合研究论文**
  - Y. Yang, K.P. Chow, Forensic Analysis of F Kong, 3-6 January 20 pp.95-106, Springer (
  - 钟琳，黎家盈，邹锦汀 场重构,《电信科学》
  - J. Fang, Z. Jiang, S.M Dual Cube Hashing S Proceedings of the six Approaches to Digital California, USA, 2011
  - R. Xu, K. P. Chow, Y. International Compute
  - J. Fang, Z. Jiang, K.P based Chinese Shanz IFIP WG 11.9 Interna South Africa, 2012, A



- 山东科学院的山东省计算中心
- 中国科学院高能物理研究所网络安全實驗室
- 重庆邮电大学
- 山东科学院,网络安全實驗室,国家超算济南中心
- 哈尔滨工业大学

Cases we have handled

- Internet child pornography case 2005
- Software copyright case in 2006
- Data leakage cases using Foxy 2008
- Internet fraud case in 2009
- Corporate internal investigation 2010
- Corporate insider theft 2011
- …

Our students – besides research

- Incoming students: mature and responsible, ethical and integrity, professional
- Professional development
  - Real case handling
  - Expert report preparation
  - Court appearance
  - Work with forensic scientists
- Our graduates
  - Law enforcement agencies
  - Private practice in digital forensics, expert witness
  - University

计算机取证 – 国际合作

- 研究应用在分析电子罪行的贝叶斯网络(Bayesian network)
  - 伙伴: Dr. Overill of 伦敦大学国王学院
- 协办国际会议
  - 第六届IFIP WG 11.9数字取证国际会议于2010年1月3日至6日在香港大學举行
    - http://www.ifip119.org
- ICDFI 2012 : The First International Conference on Digital Forensics and Investigation, Beijing, China, 21-23 Sep 2012

Publications:
IEEE Transactions, Eurocrypt, ACNS, ACISP, ….
Quite a few were awarded "Best paper award"

Funding:
Research funding, e.g. AoE, CRF
香港特别行政区，创新科技基金,
Contract research

Due to the time limit, may be we can share other projects and photos next time.

<Thank you>
<谢谢>