CONFERENCE ATTENDANCE REPORT
- HICSS 2016 -

Jan 5~8, 2016

Ae Ri Lee, Ph.D.

Research Professor, Barun ICT Research Center, Yonsei University

(**sharon@barunict.kr**)

Table of Contents

- About HICSS

- Conference Schedule

- Scenes at HICSS 2016

- Introduction of Interesting Research in HICSS

  – Research on Cause & Effect of Changes in Privacy Policies :
    Why Companies Change Privacy Policies: A Principal-Agent Perspective

  – Research on Developing Measurement of Factors in Information
    Security & Privacy :
    Measuring the Human Factor in Information Security and Privacy

  – Research on Smartphone Addiction :
    The Impact of Mere Exposure Effect on Smartphone Addiction

About HICSS

http://www.hicss.org/

- The Hawaii International Conference on System Sciences (HICSS) is an annual conference for Information Systems and Information Technology academics and professionals since 1968

- Along with ICIS, HICSS is widely considered to be one of the most prestigious international conferences for IS/IT in the world

- The conference, which now draws over 1,000 participants every year, presents a platform for sharing recent IS research and panel discussions via symposia, workshops, and tutorials

- HICSS provides a unique and highly interactive environment for researchers to exchange perspectives and ideas in various areas of information, computer, and system sciences

- The 49th Annual HICSS 2016 was held in Kauai, technically supported by IEEE Computer Society

Conference Schedule

HICSS-49
HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES
5-8 January 2016, Kauai, Hawaii

- Schedules
  - 1/5 : Attended Symposium, Workshop & Tutorials on
    - ✓ Cybersecurity in Action, Social Network Analysis, and Collective Intelligence & Crowdsourcing
  - 1/6 : Attended Research Paper Sessions on
    - ✓ Innovative Behavioral IS Security & Privacy Research, Resilience against Crises & Disasters using IS, and Social & Psychological Perspectives in IS Collaboration
  - 1/7 : Attended Research Paper Sessions on
    - ✓ Information Security & Privacy, Digital Innovation, and Social Media & Enterprise
  - 1/8 : Attended Research Paper Sessions on
    - ✓ Mobile Value Services (Mobile Addiction), IoT (Connecting People, Things, & Data), Cybersecurity, and IS Collaboration such as Crowdfunding
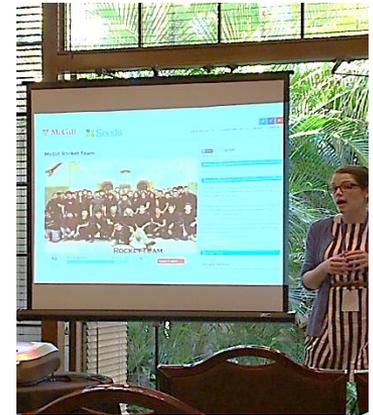
Scenes at HICSS 2016 (1/2)

- Symposium, Workshop, and Keynote Address on Jan 5~6, 2016
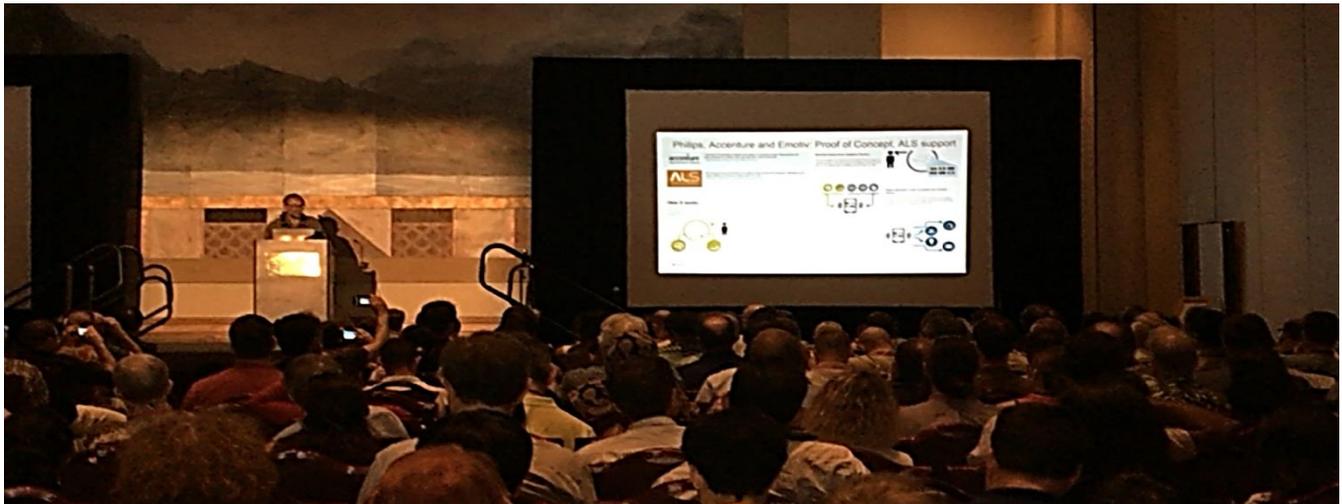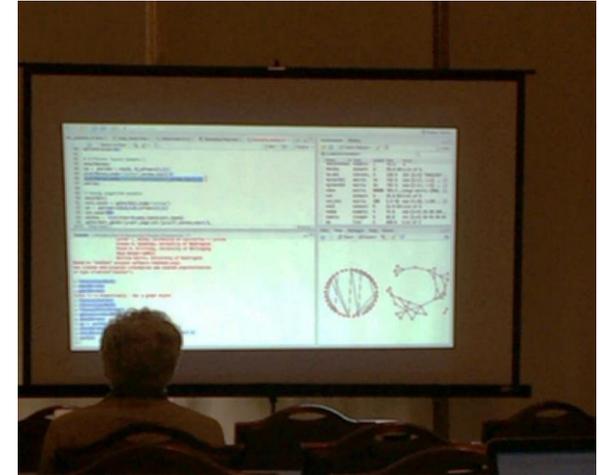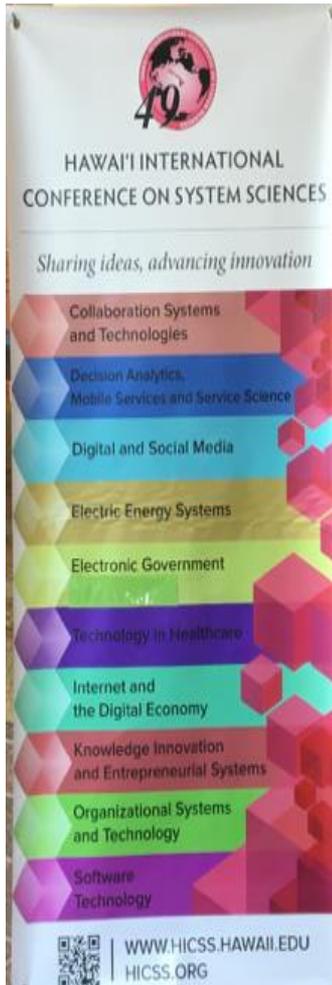
Scenes at HICSS 2016 (2/2)

- Research Paper Sessions on Jan 6~8, 2016

- Title : Why Companies Change Privacy Policies: A Principal-Agent Perspective

- Authors : Wallace Chipidza et al. (at Baylor University)

- Using a principal-agent theoretical lens, this study analyzes 218 changes to privacy policies of 5 prominent Internet companies (Amazon, Dropbox, Facebook, Google & Microsoft) over 15 years

  - ✓ 39 changes from Facebook, 50 from Microsoft, 93 changes from Google, 25 from Dropbox, and 11 from Amazon

- Findings & Results

  - ✓ Categories of privacy policy changes and their relative frequencies

Nature of Change	Description	Frequency(%)
Restrictive Changes	Any changes that increased the chances for hidden action by companies or their affiliates and third parties - Expansion of access to affiliates and non-affiliated 3rd parties; Geographical expansion; Narrowing user involvement; Personalization → more entities gain access to consumer's information	61
Empowering Changes	changes in privacy policies that strengthened user privacy : e.g.) encrypts user files on its servers by default, opt-in consent, etc.	29
Law Enforcement/ Regulatory Changes	- Legal compliance - Privacy protection and legal enforcement	7
Watchdog Monitoring Changes	- In the US, 3 major watchdogs TRUSTe, Better Business Bureau and JAMS monitor how technology companies protect customers' privacy - Companies receive a seal of approval	3

  → It found that over time, privacy policy updates are more likely to weaken, rather than strengthen, user privacy on the Internet.

- Findings & Results

  - ✓ 3 Possible reasons that organizations make changes in privacy policies based on data analyzed

    - ▪ Declines in Revenue Growth :
      The sharing or selling of data to third parties constituted a plurality of restrictive changes to privacy policies → revenue growth can be a strong motivator

    - ▪ Increasing Monetary Value of Data :
      Increasing value of data incentivizes companies to exploit the personal data within their control

    - ▪ Informing Users :
      At a minimum, the company's privacy policy must perform its intended role of narrowing the information gap by informing users of the internal policies

    - ➔ Results show that companies are more likely to update their privacy policies if they experience negative revenue growth over successive financial reporting periods

  - ✓ Results show that changes in privacy policies benefit companies at the expense of user privacy, we conclude that the principal-agent problem (i.e., the agent will aim to maximize his self-interest If the principal is unable to monitor the actions of the agent) exists in the information privacy arena

- Title : Measuring the Human Factor in Information Security and Privacy

- Authors : Marc J. Dupuis et al. (at University of Washington)

- This paper develops and validates of survey instruments designed to measure the human factor in information security and privacy

- The instruments are intended to measure the extent to which people engage in the responses necessary to mitigate 3 different information security and privacy threats: computer performance compromise, personal information compromise, and loss of data and files

- Findings & Results

  ✓ Results of Literature Search on Information Security Response

Information Security Response	Source(s)
Backup Data and Files	(Aytes & Connolly, 2004; Crossler & Bélanger, 2010; Ng & Rahim, 2005)
Computer Maintenance	(Crossler & Bélanger, 2010)
Educate Others in Home	(Crossler & Bélanger, 2010)
Information Sharing Selectivity	(Fogel & Nehmad, 2009; D. Shin, 2010; Youn, 2005)
Network of Friends/ Connections Selectivity	(Fogel & Nehmad, 2009; D. Shin, 2010; Youn, 2005)
Password and Username Usage	(Crossler & Bélanger, 2010; Yan, Blackwell, Anderson, & Grant, 2005)
Scan Computer for Malware	(Crossler & Bélanger, 2010; Furnell et al., 2006; Johnston & Warkentin, 2010; Ng & Rahim, 2005)
Setup Computer Permissions	(Crossler & Bélanger, 2010)
Setup Wireless Network Securely	(Crossler & Bélanger, 2010; Klasnja et al., 2009; Woon et al., 2005)
Software Updates	(Crossler & Bélanger, 2010; Furnell et al., 2006)
Use Caution When Following Links in Email	(Crossler & Bélanger, 2010; Dhamija et al., 2006; Downs et al., 2007)
Use Caution When Providing Personal Financial Information	(Cazier & Medlin, 2006; Crossler & Bélanger, 2010; Mannan & van Oorschot, 2008)
Use Firewall	(Crossler & Bélanger, 2010; Furnell et al., 2006)

YONSEI UNIVERSITY

Barun ICT Research Center

- Findings & Results

  - ✓ Threat-Response Pairs

Threats and their Associated Responses	Number of Indicators
1. Computer Performance Compromise	7 indicators
Computer Maintenance	1 indicator
Scan Computer for Malware	3 indicators
Software Updates	2 indicators
Use Firewall	1 indicator
2. Personal Information Compromise	26 indicators
Educate Others in Home	1 indicator
Information Sharing Selectivity	5 indicators
Network of Friends/ Connections Selectivity	2 indicators
Password and Username Usage	6 indicators
Scan Computer for Malware	3 indicators
Setup Wireless Network Securely	2 indicators
Use Caution When Following Links in Email	3 indicators
Use Caution When Providing Personal Financial Information	3 indicators
Use Firewall	1 indicator
3. Loss of Data and Files	9 indicators
Backup Data	2 indicators
Educate Others in Home	1 indicator
Scan Computer for Malware	3 indicators
Setup Computer Permissions	2 indicators
Use Firewall	1 indicator

Barun ICT
Research Center

- Findings & Results

  - ✓ E.g.) Developed Instrument of Personal Information Compromise

Indicator	Conditional	Question Text
Educate 1	Additional option provided: *N/A – I live alone.*	I am confident that someone in my home (i.e., you, someone else) regularly educates others in the home about proper information security behaviors.
Malware 1	Operating System (OS) is Windows	I am confident that my primary computer has anti-malware software that is updated automatically on a weekly or more frequent basis.
Malware 2	Operating System (OS) is Windows	I am confident that my primary computer is automatically scanned for malware in real-time (e.g.,
Firewall 1	None	I am confident that I have a firewall enabled for my primary computer.
Wireless 1	None	I am confident that my wireless network is using some type of encryption.
Wireless 2	None	I am confident that the default password on the device (e.g., router) I use for wireless access to the Internet has been changed.
Passwords 1	None	I am confident that I use long and complex passwords for important logins.
Passwords 2	None	I am confident that my passwords for less important logins are NOT the same as those for important logins.
Email 1	None	I very rarely, if ever, click on the links in emails I receive.
Email 2	None	If I were to click on a link in an email I received, I would check to make sure that the link goes to a site that appears legitimate.
Financial 1	Additional option provided: *N/A – I do not store my personal financial information online.*	I only store my personal financial information on websites that I do regular business with.
InfoShar 1	None	I am careful about the information I make public on the Internet.
Connections 1	None	I am selective in who I choose to be a friend/connection with on social networking sites.

  - ✓ Further detail : http://faculty.washington.edu/marcjd/data

Barun ICT
Research Center

- Title : The Impact of Mere Exposure Effect on Smartphone Addiction

- Authors : Chongyang Chen et al. (at University of Science and Technology of China)

- This paper investigates whether and how extensive exposure motivates users to use smartphone addictively from the lens of mere exposure effect.

- Based on the mere exposure effect theory, It proposes convenience, habit and enjoyment to describe the mere exposure effect, as well as incorporating concentration into the research model

  ✓ More Exposure Effect (MEE) Theory :

    ▪ MEE is a well-known phenomenon in social psychological research

    ▪ MEE denotes that favorable feelings may automatically arise in the appearance of exposure to repeated stimuli. That is, stimuli which are easy to be observed and take place frequently are more likely to result in positive affection

    ▪ A reasonable explanation may be that human beings prefer minimizing the cognitive load of processing information : Familiar information is easier and more fluent for people to process; The acquisition of practiced skills specific to an activity via the repeated experience will reduce efforts

    ▪ MEE simply points out such effects through affective reaction, which overlooks non-affective outcomes

- Research method : survey

  - ✓ Smartphone addiction Measure :

    - Using my smartphone sometimes interferes with other (e.g., work or study).

    - My social life has sometimes suffered because of using my smartphone.

    - When I am not using my smartphone, I often feel agitated.

    - I have made unsuccessful attempts to reduce the time using my smartphone.

    - I find it difficult to control my smartphone use

  - ✓ Habit Measure :

    - Using my smartphone has become automatic to me.

    - Using my smartphone is natural to me.

    - When I want to interact with friends and relatives, using my smartphone is an obvious choice for me.

YONSEI UNIVERSITY

Barun ICT Research Center

- Findings & Results
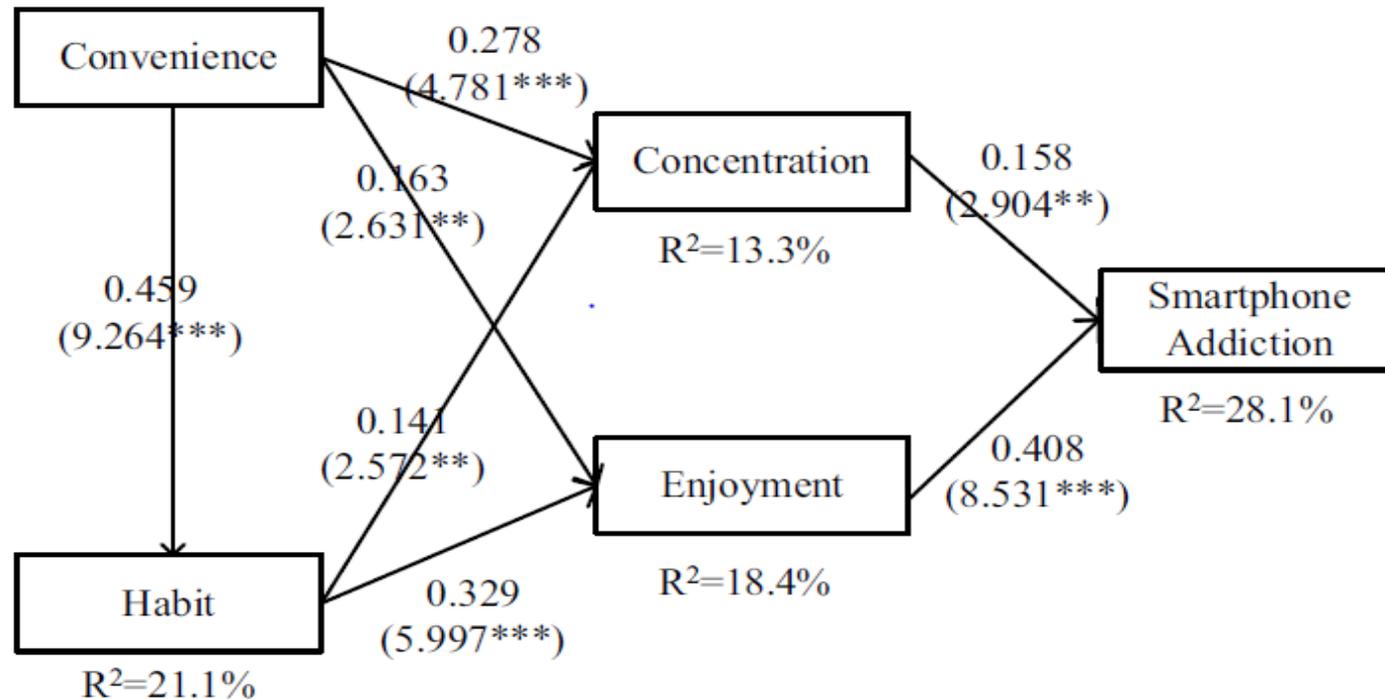
➔ Results shows that convenience facilitates the formation of habit and drives higher degrees of concentration and enjoyment; Habit also generates users' reactions of concentration and enjoyment, which further result in smartphone addiction.

Thank You