Does Context Influence Responses to Firewall Warnings?

Muhammad Mahmoud,
Sonia Chiasson, Ashraf Matrawy
Carleton University, Ottawa Canada

APWG
Unifying the
Global Response
to Cybercrime

Security Warnings

- Front-line defense against online cyber security threats
- Warnings unlikely to ever completely disappear
  - Situational/social dependencies, end-user values, automation failures
- Previous studies look at the *content* of security warnings (SSL, firewall)

2

APWG
Unifying the
Global Response
to Cybercrime

Botnet Mitigation

- Botnets responsible for spam, online phishing, adware, spyware, DDoS attacks
- Previous work in disrupting botnet IRC command and control communications
  - Relies on interrupting communication and asking the user to confirm whether this communication was initiated/trusted.

3

APWG Unifying the Global Response to Cybercrime

Research Questions

With respect to firewall warnings:

- **RQ1:** Does the ***context*** of what the user is doing affect his/her response to the warning messages? Does the ***content*** of the message affect responses?
- **RQ2:** Do users understand the warning messages and the risks in ignoring them?

4

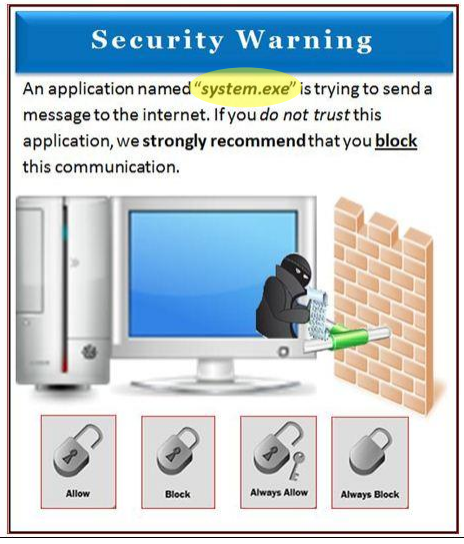
APWG Unifying the Global Response to Cybercrime

Study Design

- 56 participants, primarily students, aged 19 to 50+
- Self-rated computer expertise = mean 3.4 of 5
- Online questionnaire with 9 scenarios
- Online questionnaire instead of full study to inform design of future system

5

Consider a scenario where while you are using ***MS Word***, Internet security software popped up the following warning messages.

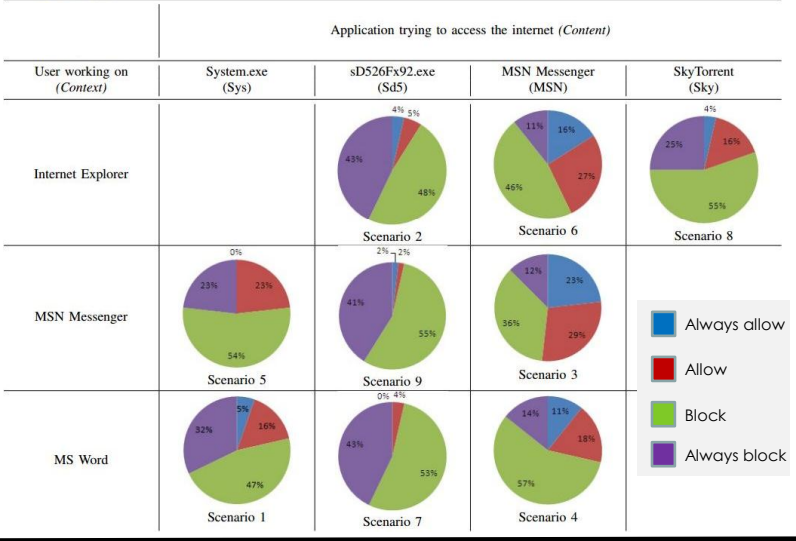


9 Scenarios

- 3 applications (***Context***):
  - Internet Explorer
  - MSN Messenger
  - MS Word
- 4 warnings (***Content***)
  - System.exe
  - sD526Fx92.exe
  - MSN Messenger.exe
  - SkyTorrent.exe

6

User Decisions



eCrime '12 Puerto Rico October 22-25 APWG
APWG Unifying the Global Response to Cybercrime

RQ1: Effect of Content and Context

- Friedman's test and post-hoc Wilcoxon Rank Sum test show
  - a statistically **significant effect of the content** of the warning on user responses of whether to allow access to the internet.
  - **No significant differences for the application context** on user responses

eCrime '12 Puerto Rico October 22-25 APWG
APWG Unifying the Global Response to Cybercrime

RQ2: User understanding of risks

- Users' free-form responses indicate that users were aware of content and context of messages
- Users could explain meaning of warnings
- 80% of users reported reading most of each message
- 90% at least partially understood the warning
- Users were most suspicious about sD526Fx92.exe
- 93% wanted some involvement in decision-making process, but < 5 warnings per week

9

APWG Unifying the Global Response to Cybercrime

Conclusions

- ***Context*** of when message appears does not matter
- ***Content*** of the warning does matter
- Users ***understood*** need for warnings, ***reasonable mental models*** of the risks
- Users willing to respond to ***infrequent*** warnings only

10

APWG Unifying the Global Response to Cybercrime

Questions/Comments?

- Contact authors:
  - mimam@sce.carleton.ca
  - chiasson@scs.carleton.ca
  - amatrawy@sce.carleton.ca

11

APWG Unifying the Global Response to Cybercrime