Insights into User Behavior in Dealing with Internet Attacks

Northeastern University
Boston

Bilkent University
Ankara

Eurecom
Sophia Antipolis

Kaan Onarlioglu, Utku Ozan Yilmaz,
Engin Kirda, Davide Balzarotti

Problem

Exploit link	⇒	Click
Risky file	⇒	Download
Malware	⇒	Run
Warning Message	⇒	Dismiss

Interaction: “Human Aspect”

Previous Work

- How do attackers trick users?
- What techniques do they use?
- How successful are they?
  - [Dhamija, CHI ‘06]
  - [Sunshine, SSYM ’09]
  - [Egelman, CHI’ 08]
  - [Friedman, CHI ‘02]
  - ….and many more
- Usability of security solutions…

Our Questions

- How do users react to current threats?
  - XSS, session fixation, exploit links, file-sharing scams, malicious trick banners
- …evaluate security implications of actions?
- …assess the risk?

Experiment

- Online test system

- 44 security-related scenarios in 3 suites
  - Web attacks
  - Email attacks
  - File-sharing attacks

Contributions

- 164 participants
- Largest study on prevalent attacks

- Gain insights into ‘Perception’ & ‘Security’
- Understand decision-making cues
- Identify attack vectors

Experiment Design

- Perception Score
  - "How dangerous or safe do you think clicking on this link is?"
- Security Score
  - "Would you click on this link?"

- "Please explain your reasoning."

Web Attacks

- XSS, session fixation, link manipulation tricks

Hey, check this article out, great stuff!

http://example.blog.com/show.php?title=%22%3E%3Cscript%3Edoc
ument.location%3D%27http%3A%2F%2Fwww.cgisecurity.com%2Fcgi-b
in%2Fcookie.cgi%3F%27+%2Bdocument.cookie%3C%2Fscript%3E

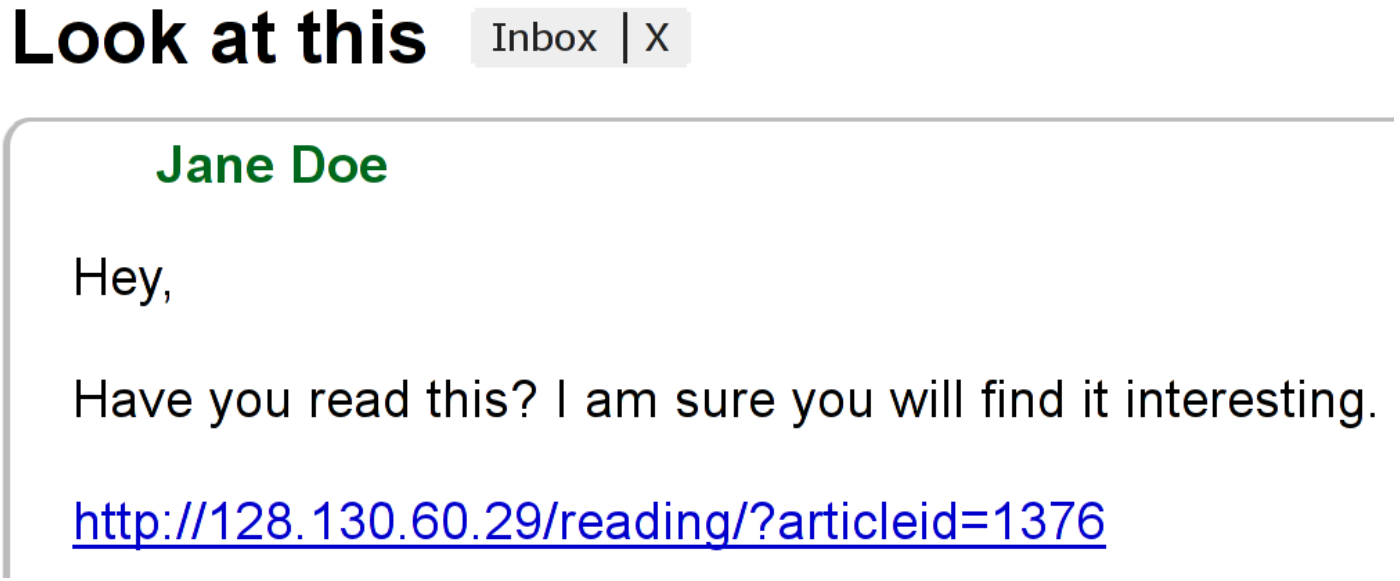
> **http://example.blog.com/show.php?title=%22%3E**
> **%3Cscript%3Edocument.location%3D%27http%3A%2F**
> **%2Fwww.cgi**
> example.blog.com

Web Attacks

- Benign URLs:
  - http://www.amazon.com/software-business-education-finance-childrens/b/ref=sa_menu_sw4/178-3182747-8297639?ie=UTF8&node=229534
- Raw IP address
- TinyURL
  - Destination?

Email Attacks

- .exe attachment, phishing, 419 scam, prize giveaway, newsletters, banking…



File-Sharing Attacks

- BitTorrent
  - The Pirate Bay, Torrentz, isoHunt
- OCH:
  - Filesonic, Filestube, Megaupload/video, iFolder

- Cues:
  - Filename, download contents, size, date, uploader, comments, extensions, …

Nosferatu [Full DOWNLOAD]

Sponsored results

New! - **How To Get One Access To ALL Download Sites?**

Also try: **nosferatu** **nosferatu** eine symphonie des grauens **nosferatu** megaupload **nosferatu** rapidshare com **nosferatu** Movie **nosferatu** download

Nosferatu
filesonic.com ext: **.mp4** size: 699 MB date: 2010-08-30
☆☆☆☆☆ **Nosferatu**
http://www.filesonic.com - Download

Nosferatu
4shared.com ext: **.exe** size: 701 MB date: 2011-01-21
☆☆☆☆☆ **Nosferatu**
http://search.4shared.com/q/BFACAw/1/nosferatu - Download

Nosferatu 1922 F W Murnau
uploadbox.com ext: **.rar** parts: 6 size: 1.20 GB date: 2011-02-07
☆☆☆☆☆ **Nosferatu** 1922 F W Murnau
http://uploadbox.com - Download

Nosferatu 1922
4shared.com ext: **.rar** size: 790 KB date: 2010-08-31
☆☆☆☆☆ **Nosferatu** (1922)
http://search.4shared.com/q/AigCAw/1/nosferatu - Download

Trackers: (aggregated from BitTorrent sites everywhere for reliability and speed)

tracker1.publicbt.com:80/announce: 19 seeds
trfkad.tracker.prq.to:80/announce: 16 seeds
tracker-torrentsbyrizzo.info:80/announce: 16 seeds
t1.pow7.com:80/announce: 14 seeds
torrentbay.to:6969/announce: 11 seeds
tracker2.istole.it:80/announce: 9 seeds
genesis.1337x.org:80/announce: 5 seeds
94.228.210.41:6969/announce: 4 seeds
inferno.demonoid.com:3408/announce: ? seeds

Uploader's Comments:
[Find more at http://www.torrentportal.com]

Directory: Nosferatu.XviD

Files:

codecs.exe	1.2 MB
download_codecs.lnk	4.0 KB
download_free_movies.html	13.2 KB
Nosferatu.avi	700.24 MB
README.txt	550 bytes
subtitles.lnk	4.0 KB

***700.65 MB** in **6** files. Torrent created **187.2 weeks** ago.*

info_hash: 8a9a3be374c9af295ed7280acf18cc2f5cc36eff (?) | BTID: 119663733 | **Permalink**

Nosferatu 1922 F W Murnau

Sponsored link: Nosferatu__1922__F.W._Murnau.rar [FAST DOWNLOAD]

Download now from uploadbox.com:

Nosferatu__1922__F.W._Murnau.rar 699 MB Download

Total size: **699.62 MB**

New! - REGISTER FOR FREE and get ONE cheap ACCESS TO FILE SHARING SITES

Direct links:

```
http://uploadbox.com/files/64354de3d0?affil=1
```

Sponsored link: Nosferatu__1922__F.W._Murnau.rar [FAST DOWNLOAD]

Password recovery: RAR Magic Password Cracker

Added: 2011-02-07 12:06:03

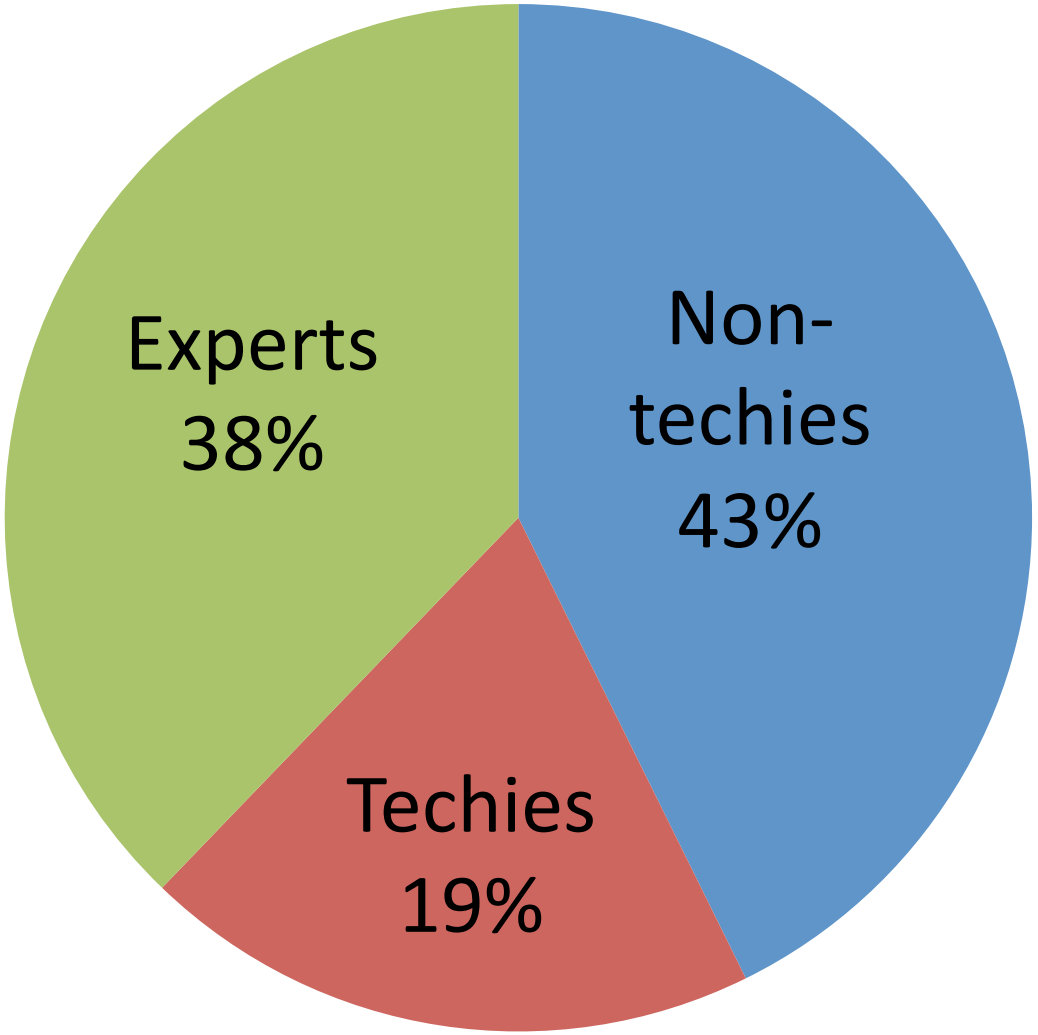
Link(s) source: http://uploadbox.com

Participants

- 164 participants:
  - Facebook, Twitter, personal contacts
- Age: 19 to 69, Mean: 26.5
- 17 nationalities

- CS, Engineering, Law, Medicine, Geology…
- PhD, Master, Bachelor, High School

Security Expertise



Total Scores

- Perception Score:
  - Experts > Techies > Non-techies
- Security Score:
  - Experts > Techies > Non-techies

[Kruskal-Wallis / Multiple comparison post-hoc tests]

- $H = 37.36$, $df = 2$, $p << 0.05$ for risk perception scores
- $H = 26.89$, $df = 2$, $p << 0.05$ for security scores

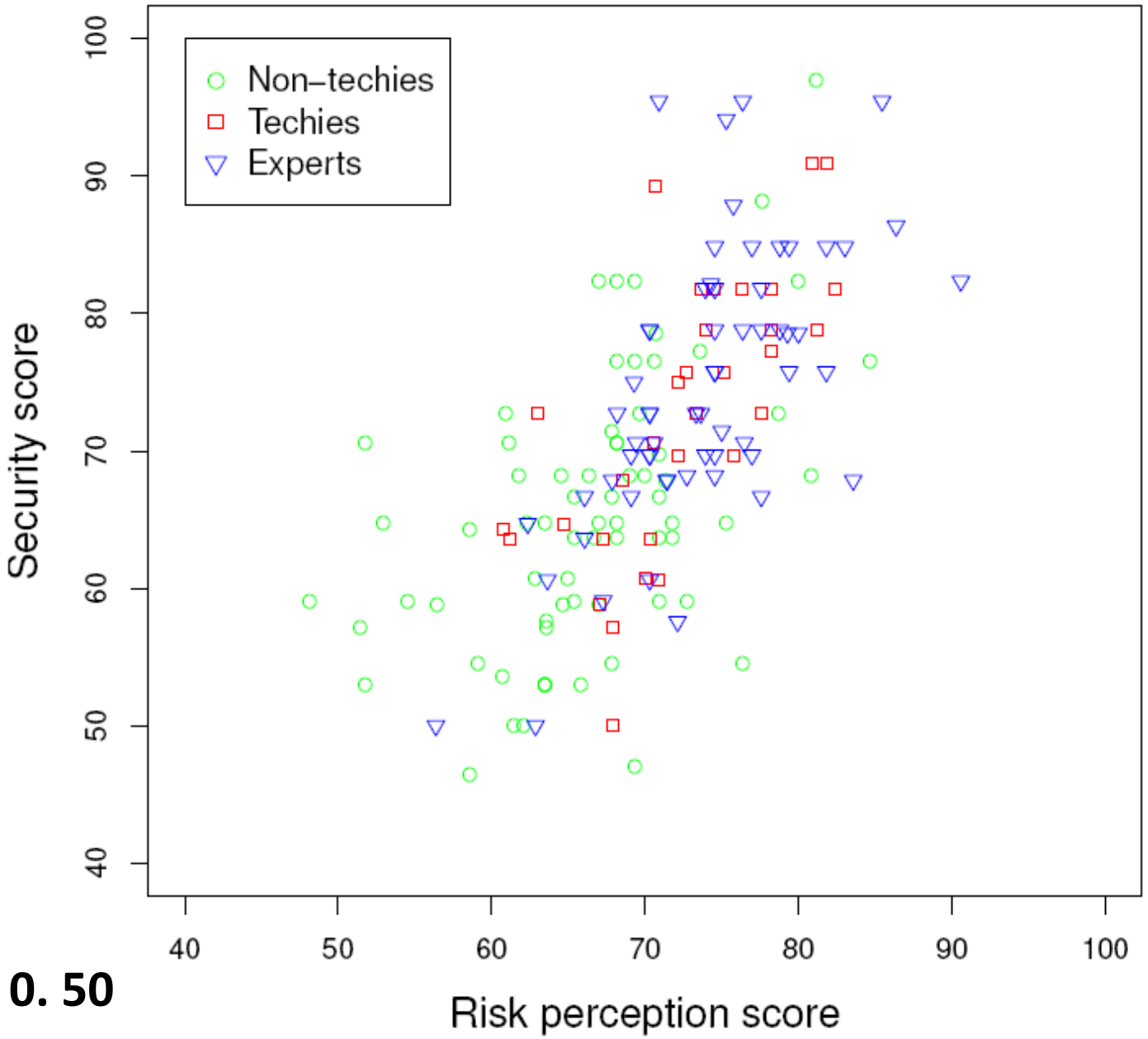
Individual Scores

- Perception Score: Experts > Non-techies
- Security Score:

  Web Attacks Suite: Experts > Non-techies

No proof that Experts > Non-techies

in Email and File-Sharing security scenarios



Non-techies: ρ = 0. 50

Rest: ρ = 0. 70

[Spearman's Rank Correlation]

Perception & Security

- Non-techies have bad perception
- …but still avert attacks!

- Exposure?
  - Spam: 95.7% Web attacks: 48.9%
  - Email attacks subverted: 97.1% by intuition
  - Can this be applied to more complex attacks?
    - Anti-Phishing Phil [Sheng, SOUPS '07]

Misleading Cues

- URL length & complexity:
  - "Too long and complicated"
  - "Many funny letters"
  - "Has a long name and unknown code in it"

- www.paypal.hostding.com:
  - "Easy to read"
  - "Clear obvious link"
  - "[Amazon link] was not like this"

Misleading Cues

- File size:
  - Movie.rar cannot be 700MB
  - 700KB movie from 1922: legit

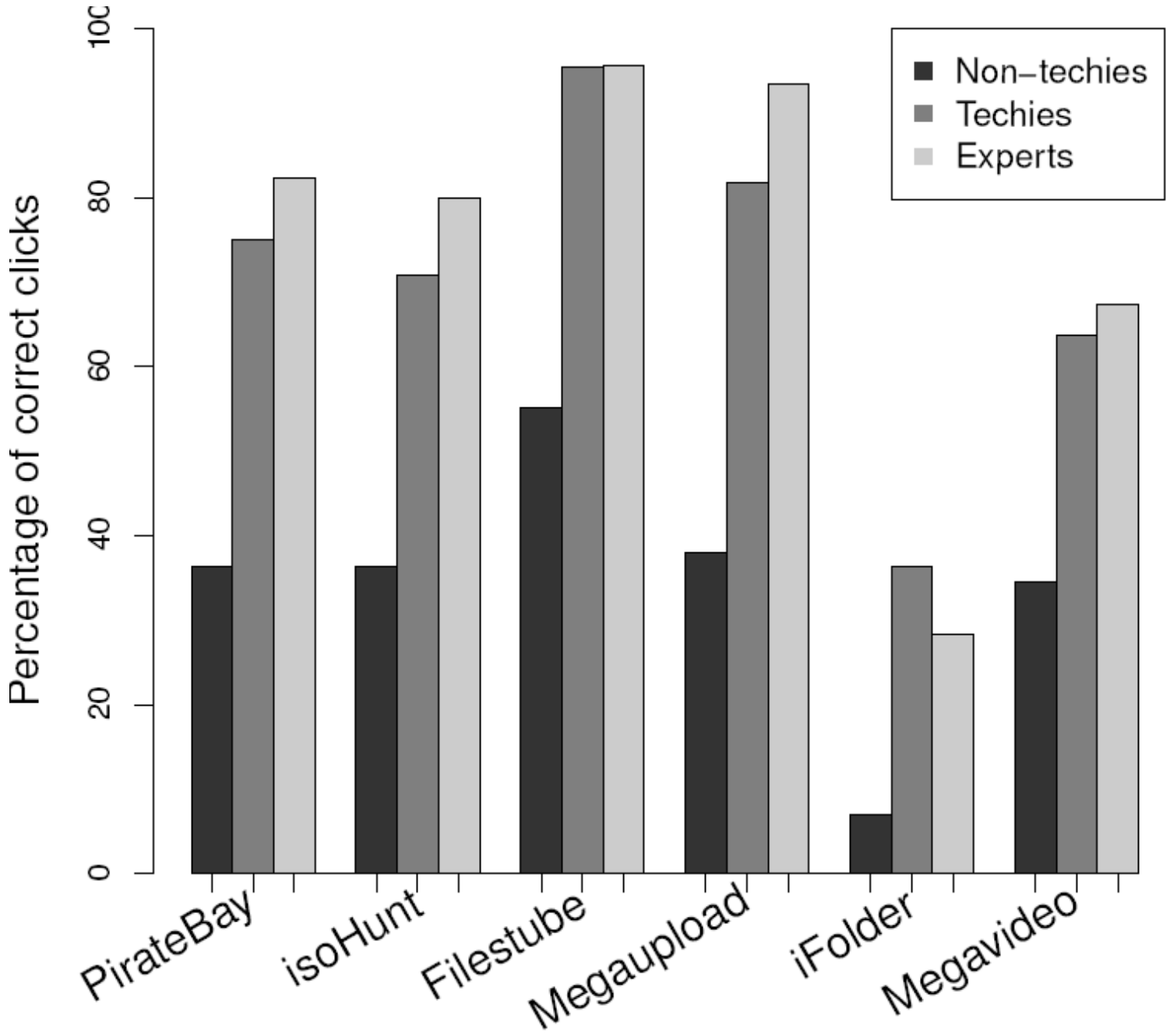
- Informed decisions not possible

  ⇒ Rely on misleading cues

Shortened URL & IP Address

	Verify destination	Not familiar
TinyURL	0%	35.7%
IP address	0%	28.6%

- YouTube video
- Index of photographs
- Blog article
- Printer interface
- Proxy code
- Router configuration


Percentage of correct clicks
0
20
40
60
80
100
Non−techies
Techies
Experts
PirateBay
isoHunt
Filestube
Megaupload
iFolder
Megavideo

Conclusions

- Online test system, prevalent attacks
- 164 participants, largest study to date

- Perception ≠ Security
- Size and length: bad cues
- Shortened URLs: Tools, but no awareness
- Trick banners: Serious business

Thank you!

Q & A