

How to Hack the Microsoft Research Conference Management Tool (MSRCMT)

***Raphael C.-W. Phan**

Information Security Research (iSECURES) Laboratory,
Swinburne University of Technology (Sarawak Campus), Malaysia

Huo-Chong Ling

Center for Cryptography & Information Security (CCIS),
Multimedia University, Malaysia

About the MSRCMT

MSRCMT

— Online submission

- Personal author details
- Keep track of submissions

Conferences using the MSRCMT

Springer LNCS

- Info Hiding Workshop (IH 04)
- Int Workshop on Digi Watermarking (IWDW 04)
- Int XML Db Symp (Xsym 04)

IEEE

- Int Conf on Data Eng (ICDE 04)
- Symp on Info Visualization (InfoVIS 03)
- Workshop on Internet Apps (WIAPP 03)
- Conf on S/w Arch (WICSA 04)
- Int Conf on Comp Sys & Apps (AICCSA 05)

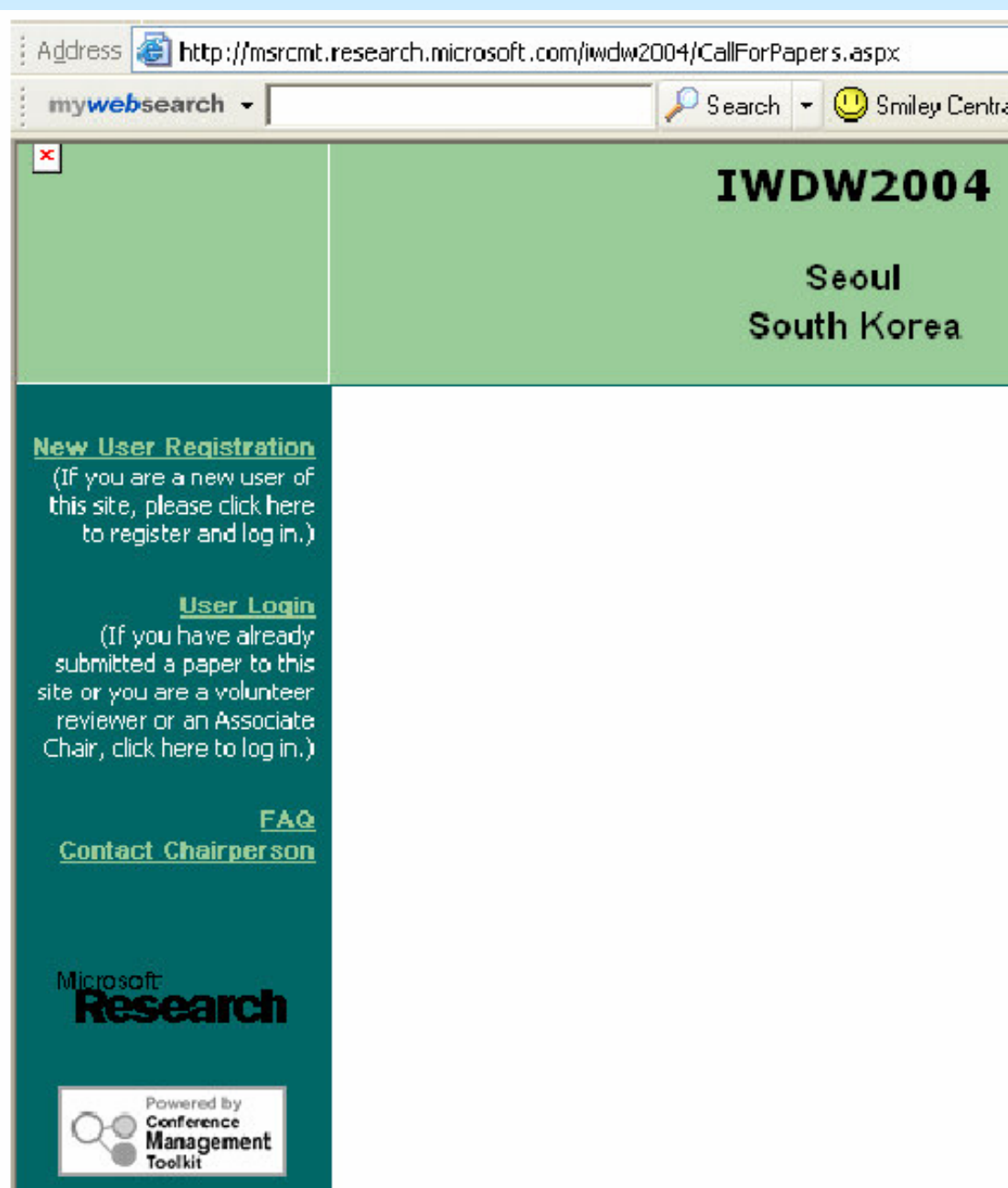
Conferences using the MSRCMT

ACM

- Conf on E-Commerce (EC 04)
- SIGMOD Workshop on ... Data Mining & K Discovery 03
- Symp on Theory of Computing (STOC 04)
- Workshop on Data Eng for Wi & M Access (MobiCom 03)

How it happened

- Wanted to submit to IWDW 2004
- I registered, keyed in
 - My details, password
 - co-author details, email



The screenshot shows a web browser window with the address bar containing the URL <http://msrcmt.research.microsoft.com/iwdw2004/CallForPapers.aspx>. The page has a green header with the text "IWDW2004" and "Seoul South Korea". Below the header, there are several links: "New User Registration" (with a subtext: "(If you are a new user of this site, please click here to register and log in.)"), "User Login" (with a subtext: "(If you have already submitted a paper to this site or you are a volunteer reviewer or an Associate Chair, click here to log in.)"), "FAQ", and "Contact Chairperson". At the bottom, there is a Microsoft Research logo and a logo for "Powered by Conference Management Toolkit".

How it happened



The screenshot shows a web browser window with the URL <http://msrcmt.research.microsoft.com/iwdw2004/login.aspx>. The page title is "International Workshop on Digital Watermarking". The main heading is "IWDW2004" with the location "Seoul South Korea".

On the left sidebar, there are links for "User Registration", "User Login", "FAQ", and "Contact Chairperson".

The main content area is titled "User Login:" and contains the following text: "Enter your e-mail address and password below to add, delete or view your account. If you have forgotten your password, click **E-mail My Password**. Your e-mail address will be sent to you." Below this text are two input fields: "E-mail address:" and "Password:". A "Login" button is positioned below the password field, and an "E-mail My Password" button is located at the bottom right of the form area.

How it happened

- Login requires
 - Email address (login ID)
 - Password
- Login allows
 - Add new papers
 - View/edit current papers
 - View/edit personal details

How it happened

- ✿ What about co-authors?
 - Account auto-created, password is 0!
 - Co-author can request for this to be sent to him

Further probing

- How about co-authors of other papers we dunno?
- 1. IWDW 2003 programme \Rightarrow past non-first authors
- 2. Searched for emails
- 3. Logged in with emails and password 0
 - \Rightarrow We got 5 successful logins!
 - \Rightarrow They were again non-first authors this year, & their accounts auto-generated, and given password 0!
- Repeated for another conference, also successful

Lessons

- ✿ What goes wrong usually?
- ✿ Implementors \neq cryptographers (Generally)
 - Crypto concepts not well understood
 - Good designs poorly implemented
- ✿ Security engineering
 - Requirements \rightarrow design \rightarrow implementation \rightarrow application
 - Each link is equally important

Thanks

- ✿ Ross Anderson, Niels Ferguson, Burt Kaliski Jr, John Kelsey, Paul Kocher, Serge Vaudenay for interest & comments.