(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 359 491 A8

(12) **CORRECTED EUROPEAN PATENT APPLICATION**
Note: Bibliography reflects the latest situation

(15) Correction information:
Corrected version no 1 (W1 A1)
INID code(s) 71,72

(48) Corrigendum issued on:
21.07.2004 Bulletin 2004/30

(43) Date of publication:
05.11.2003 Bulletin 2003/45

(21) Application number: **03008063.4**

(22) Date of filing: **14.04.2003**

(51) Int Cl.[7]: **G06F 1/00**, H04L 29/06
// H04L9/32

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT RO SE SI SK TR
Designated Extension States:
AL LT LV MK

(30) Priority: **30.04.2002 US 135043**

(71) Applicant: **MICROSOFT CORPORATION**
Redmond, Washington 98052 (US)

(72) Inventors:
- **Ayyagari, Arun**
  Seattle, Washington 98115 (US)
- **Ganugapati, Krishna**
  Redmond, Washington 98053 (US)
- **Simon, Daniel R.,**
  Redmond, Washington 98052 (US)
- **Moore, Timothy M.**
  Bellevue, Washington 98008 (US)
- **Bahl, Pradeep**
  Redmond, Washington 98053 (US)

(74) Representative: **Grünecker, Kinkeldey,**
Stockmair & Schwanhäusser Anwaltssozietät
Maximilianstrasse 58
80538 München (DE)

(54) **Methods for remotely changing a communications password**

(57) Disclosed are methods for an authentication client, having been authenticated by an authentication server, to leverage the effects of that authentication to implement a new communications password. The authentication client gets a new password from its user. From the new password and from information provided by the authentication server, the authentication client derives a "password verifier." The password verifier is then shared with the authentication server. The new password itself is never sent to the authentication server, and it is essentially impossible to derive the new password from the password verifier. The authentication client and the authentication server, in parallel, derive a new set of authentication and encryption security keys from the new password and from the password verifier, respectively. This process may be repeated to limit the amount of data sent using any one particular set of security keys and thus to limit the effectiveness of any statistical attacker.

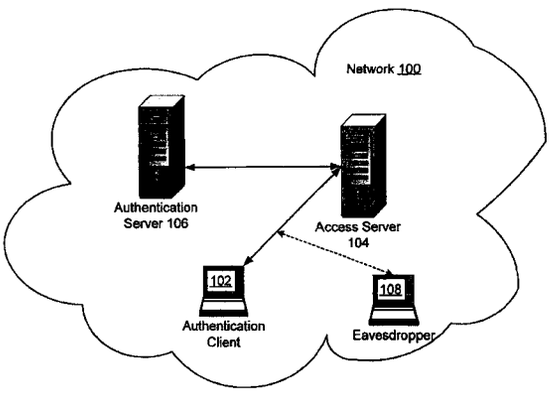

FIG. 1

EP 1 359 491 A8