

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局



(10) 国际公布号
WO 2022/199292 A1

(43) 国际公布日
2022 年 9 月 29 日 (29.09.2022)

(51) 国际专利分类号:
G06F 21/56 (2013.01)

(21) 国际申请号: PCT/CN2022/076785

(22) 国际申请日: 2022 年 2 月 18 日 (18.02.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202110323745.1 2021 年 3 月 26 日 (26.03.2021) CN

(71) 申请人: 支付宝 (杭州) 信息技术有限公司 (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) [CN/CN]; 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。

(72) 发明人: 曹世杰 (CAO, Shijie); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。 李文杰 (LI, Wenjie); 中国浙江

省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。 赵豪 (ZHAO, Hao); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。

(74) 代理人: 北京博思佳知识产权代理有限公司 (BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION); 中国北京市海淀区上地三街 9 号嘉华大厦 B 座 409, Beijing 100085 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK,

(54) Title: DETECTION OF MALICIOUS BEHAVIOR OF APPLLET

(54) 发明名称: 小程序恶意行为检测

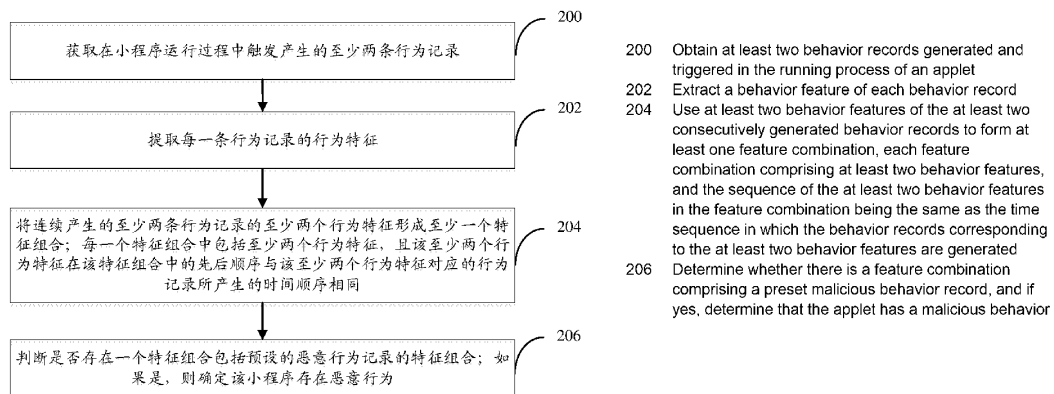


图 2

(57) Abstract: Provided are a method and apparatus for detecting a malicious behavior of an applet. The method of embodiments comprises: first, obtaining at least two behavior records generated and triggered in the running process of an applet (200); then extracting a behavior feature of each behavior record (202); next, using at least two behavior features of the at least two consecutively generated behavior records to form at least one feature combination, each feature combination comprising at least two behavior features, and the sequence of the at least two behavior features in the feature combination being the same as the time sequence in which the behavior records corresponding to the at least two behavior features are generated (204); and finally, determining whether there is a feature combination comprising a preset malicious behavior record, and if yes, determining that the applet has a malicious behavior (206).

[见续页]

SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区
保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ,
NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM,
AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG,
CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU,
IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,
RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI,
CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告 (条约第21条(3))。

(57) 摘要: 提供了一种小程序恶意行为检测方法和装置。根据实施例的方法, 首先, 获取在小程序运行过程中触发产生的至少两条行为记录 (200), 然后, 提取每一条行为记录的行为特征 (202), 接下来, 将连续产生的至少两条行为记录的至少两个行为特征形成至少一个特征组合; 每一个特征组合中包括至少两个行为特征, 且至少两个行为特征在特征组合中的先后顺序与至少两个行为特征对应的行为记录所产生的时间顺序相同 (204); 最后, 判断是否存在一个特征组合包括预设的恶意行为记录的特征组合, 如果是, 则确定小程序存在恶意行为 (206)。