New connection on: : 08-11-2017 : 22:45:09 - Last disconnection on: : 08-11-2017 : 21:13:47

V 4.0.0.44176(LP,U,linux) (Rev:41675 2016-01-15 13:33:59 +0100#(D201713)) (RPM D201713)

Welcome to EPOQUE Rebuild under the Production Environment

[EPODOC: SS 16] (natural and language and processing and certification)

Results in EPODOC **1**

[SS 17] ..v

[EPODOC: SS 17] ..fi pantenw

Unknown database/cluster. Use the command ..FI (CL) in order to check the name of the databases/clusters available. *ERROR(-50416)*

[SS 17] ..fi patenw

Database: PATENW

[PATENW: SS 1] 16

No Search Statement exists for this database. Perform first a query. *ERROR(-100813)*

[SS 1] (natural w language) and processing and certific+

Results in PATENW **3.247**

[SS 2] /IC G06F21/57

Results in PATENW **8.229**

[SS 3] 2 and 1

Results in PATENW **12**

[SS 4] ..v

[PATENW: SS 4] ..li nbdoc 10

1/12 © PATENW / EPO

PN - US2017243009 A1 20170824

PR - IN201641005995 20160222

AP - US201715438199 20170221

DT - *; Rep

CCI - G06F21/577

CCA - G06F2221/034

PA - ACCENTURE GLOBAL SOLUTIONS LTD [IE]

TI - DEVICE BASED AUTOMATED THREAT DETECTION AND RESPONSE

AB - A device may include one or more processors. The device may communicate with a set of user devices operating a set of mobile applications to obtain data regarding a set of malicious attacks associated with the set of user devices. The device may store the data regarding the set of malicious attacks via a data structure for analysis. The device may process the stored data to identify one or more vulnerabilities associated with the set of user devices or the set of mobile applications. The device may generate a security tool user interface that includes information identifying the one or more vulnerabilities associated with the set of user devices or the set of mobile applications. The device may cause the security tool user interface to be provided for display via a client device based on generating the security tool user interface.

2/12 © PATENW / EPO

PN - US2017206156 A1 20170720

PR - US201715473245 20170329; US201314019978 20130906

AP - US201715473245 20170329

DT - **

CCI - G06F21/6245

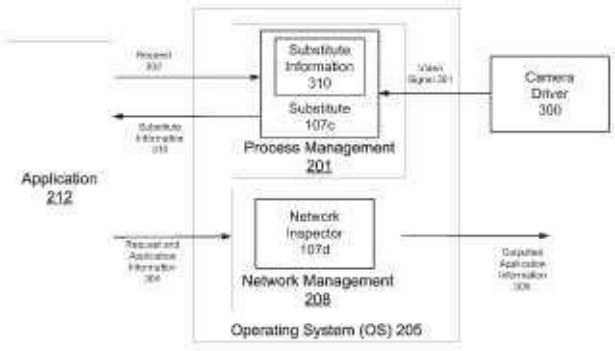
CUI - G06F11/3688 ; G06F9/54 ; G06F21/57

CCA - G06F2221/031

PA - MICROSOFT TECHNOLOGY LICENSING LLC [US]

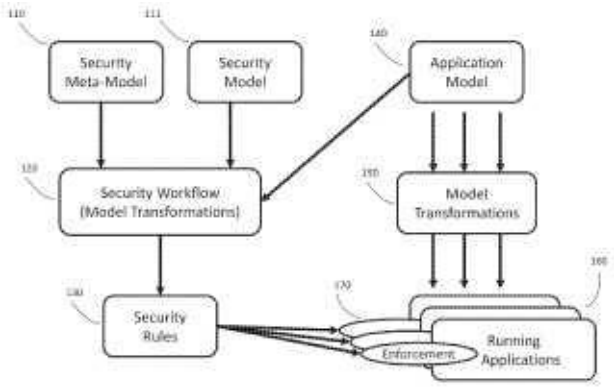
TI - VERIFICATION THAT PARTICULAR INFORMATION IS TRANSFERRED BY AN APPLICATION

AB - The technology includes a method to test what information an application transfers to an external computing device. A user's consent is explicitly obtained before the application



transfers certain types of information, such as sensitive information. When a determination is made that an application is transferring sensitive information, a prompt for consent from a user may be provided that is accurate and detailed. In pre-production environments, technology can be used to detect whether this sensitive information is being transferred, and to validate whether a prompt for consent is necessary or unnecessary. To determine this, shimming is used to intercept application calls to APIs that return sensitive information. Requested sensitive information may be substituted with recorded or forged information from those APIs to produce a sentinel or canary. Similarly, network traffic of the application may be analyzed by another shim to determine when the substitute information is present.

3/12 © PATENW / EPO



PN - US2017126741 A1 20170504

PR - US201615393975 20161229; US201514602935 20150122; US201461929987P 20140122; US201462050051P 20140912

AP - US201615393975 20161229

DT - **

CT - || R141 (A1) US9043861 B2 20150526 [ ] (LANG ULRICH [US], et al)

CCI - G06F21/604

CUI - G06F21/57 ; H04L63/20

CUA - G06F2221/034

PA - LANG ULRICH [US]; SCHREINER RUDOLF [DE]

TI - AUTOMATED AND ADAPTIVE

MODEL-DRIVEN SECURITY SYSTEM AND METHOD FOR OPERATING THE SAME

AB - A system and method for managing implementation of policies in an information technologies system receives into a processor at least one policy function stored in at least one memory, receives into the processor a policy input indicating a high-level policy for the IT system, the policy input being compliant with the at least one policy function, based on the received policy input, automatically or semi-automatically generates via the processor a rule and/or configuration by replacing at least one policy function in the policy input with the at received least one policy function, the generated rule and/or configuration being compliant with the received policy input or replacing at least one value or value placeholder in the policy input with a corresponding value, and distributes the rule and/or configuration to the at least one memory of the IT system or another at least one memory to thereby enable implementation of the policies.

4/12 © PATENW / EPO

PN - **US9465942** B1 20161011

PR - US201414459037 20140813; US201313858448 20130408

AP - US201414459037 20140813

DT - *; Rep

CT - || STSE (B1)
US8621237 B1 20131231 [ ] (BAILEY DANIEL V [US], et al);
US2008034425 A1 20080207 [ ] (OVERCASH KEVIN [US], et al);
US2008120305 A1 20080522 [ ] (SIMA CALEB [US], et al);
US2013340076 A1 20131219 [ ] (CECCHETTI ADAM [US], et al)

CCI - **G06F21/125** ; **G06F21/577** ; **G06F21/75**

CQI - G06F21/57

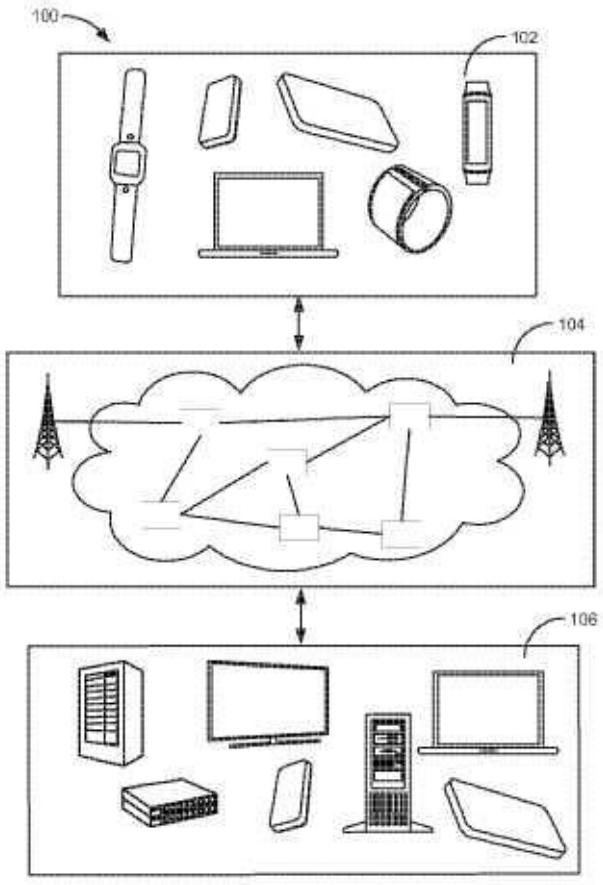
CCA - G06F2221/033

PA - AMAZON TECH INC [US]

TI - Dictionary generation for identifying coded credentials

AB - Techniques are described for identifying security credentials or other sensitive information by creating a dictionary of data elements included in documents such as source code files, object code files, or other types of files. The data elements may be identified for inclusion in the dictionary based on parsing the documents for delimiter characters, and based on the context of the data elements within the documents. The data elements may also be identified through an entropy-based analysis to detect portions of the documents exhibiting a high degree of entropy compared to a baseline entropy for the documents. The dictionary may be used in a dictionary attack against various systems to determine whether any of the data elements included in the dictionary enable access the systems. The data elements that enable access may be designated as sensitive information hard-coded into the documents.

5/12 © PATENW / EPO



PN - US2016188902 A1 20160630

PR - US201414585985 20141230

AP - US201414585985 20141230

DT - *; Rep

CT - || R141 (A1)
US2014358632 A1 20141204 [ ] (GRAFF JAMES WILLIAM [US], et al);
US2008133336 A1 20080605 [ ] (ALTMAN SAMUEL H [US], et al)

CCI - H04L67/306 ; G06F21/577 ; G06F21/6245 ; G06Q50/01 ; H04L63/20 ; H04W4/02 ; H04W4/021 ; H04W12/00 ; H04W12/02

CCA - G06F2221/034

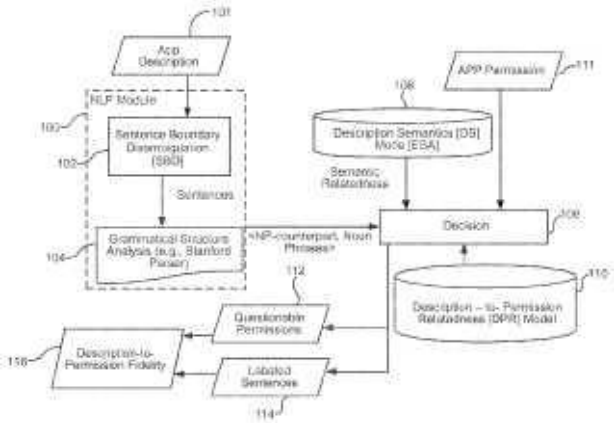
PA - SAMSUNG ELECTRONICS CO LTD [KR]

TI - COMPUTING SYSTEM FOR PRIVACY-AWARE SHARING MANAGEMENT AND METHOD OF OPERATION THEREOF

AB - A computing system includes a control unit configured to determine a usage context including a capability of a device, a usage time and a device location associated with the device, and a user context of one

or more users with access to the device; analyze a privacy risk level of a resource based on a resource content included in the resource, a metadata concerning the resource, a collective input regarding the resource, and the usage context; and generate one or more options for sharing the resource with the device based on the privacy risk level and the usage context.

6/12 © PATENW / EPO



PN - US2015332049 A1 20151119

PR - US201514711157 20150513; US201461993398P 20140515

AP - US201514711157 20150513

DT - *; Rep

CT - || R141 (A1)
US2009164926 A1 20090625 [ ] (BOYLE PETER CURRIE [CA], et al);
US8255280 B1 20120828 [ ] (KAY ERIK [US], et al);
US2012317638 A1 20121213 [ ] (CARRARA MICHAEL ANTHONY [CA], et al);
US2013212684 A1 20130815 [ ] (LI XUYANG [US], et al);
US9407443 B2 20160802 [ ] (WYATT TIMOTHY MICHEAL [US], et al);
US2014090061 A1 20140327 [ ] (AVASARALA BHARGAV R [US], et al);
US2014379521 A1 20141225 [ ] (NOVOTNY MARGARET JOANN [US], et al);
US2012124643 A1 20120517 [ ] (MORICONI MARK [US], et al);
US2012254143 A1 20121004 [ ] (VARMA KISHORE INDUKURI [IN], et al);
US8532978 B1 20130910 [ ] (TURNER RONALD C [US]);
US2013333039 A1 20131212 [

] (KELLY NICHOLAS PAUL [GB]);
US2016012220 A1 20160114 [
] (PADIDAR SASAN [US], et al)

CTNP - || R141 (A1)

[] - Costanich, Bryan. "Publishing to the App Store." Developing C# Apps for iPhone and iPad Using MonoTouch. Apress, 2011. 407-418.,

[] - Yang, Wei, et al. "Improving mobile application security via bridging user expectations and application behaviors." Proceedings of the 2014 Symposium and Bootcamp on the Science of Security. ACM, 2014.,

[] - Jing, Yiming, et al. "Riskmon: Continuous and automated risk assessment of mobile applications." Proceedings of the 4th ACM Conference on Data and Application Security and Privacy. ACM, 2014.,

[] - Zhong, Hao, et al. "Inferring resource specifications from natural language API documentation." Automated Software Engineering, 2009. ASE'09. 24th IEEE/ACM International Conference on. IEEE, 2009.,

[] - Lin, Jialiu, et al. "Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing." Proceedings of the 2012 ACM Conference on Ubiquitous Computing. ACM, 2012.,

[] - Peiravian, Naser, and Xingquan Zhu. "Machine learning for android malware detection using permission and api calls." Tools with Artificial Intelligence (ICTAI), 2013 IEEE 25th International Conference on. IEEE, 2013.,

[] - Tan, Lin, et al. "/* iComment: Bugs or bad comments?*." ACM SIGOPS Operating Systems Review. Vol. 41. No. 6. ACM, 2007.,
[] - Zhu, Jiawei, et al. "Permission-based abnormal application detection for android." International Conference on Information and Communications Security. Springer, Berlin, Heidelberg, 2012.,

CCI - G06F21/577 ; G06F21/604

CUI - G06F21/57

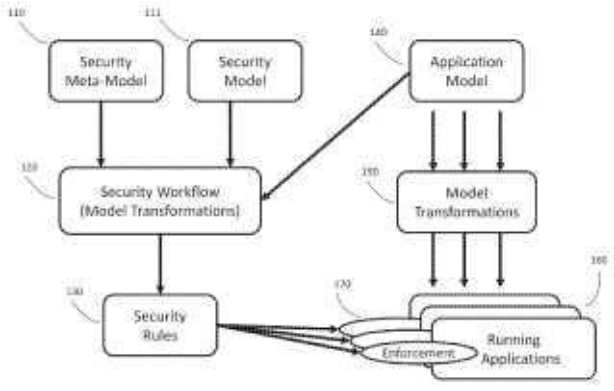
CCA - G06F2221/033

PA - UNIV NORTHWESTERN [US]

TI - SYSTEM AND METHOD FOR DETERMINING DESCRIPTION-TO-PERMISSION FIDELITY IN MOBILE APPLICATIONS

AB - A system and method are described to automatically assess description-to-permission fidelity of applications. The system and method can employ techniques in **natural language processing** and a learning-based algorithm to relate description with permissions.

7/12 © PATENW / EPO



PN - US2015269383 A1 20150924

PR - US201514602935 20150122; US201461929987P 20140122; US201462050051P 20140912

AP - US201514602935 20150122

DT - *; Rep

CT - || R141 (A1) US9043861 B2 20150526 [ ] (LANG ULRICH [US], et al)
- || STSE (B2) US9043861 B2 20150526 [ ] (LANG ULRICH [US], et al)

CCI - **G06F21/604**

CUI - **G06F21/57** ; **H04L63/20**

CUA - **G06F2221/034**

PA - (A1 B2)
OBJECT SECURITY LTD [US]

TI - (A1)
AUTOMATED AND ADAPTIVE MODEL-DRIVEN SECURITY SYSTEM AND METHOD FOR OPERATING THE SAME

- (B2)
Automated and adaptive model-driven security system and method for operating the same

AB - (A1 B2)
A system and method for managing implementation of policies in an information technologies system receives at least one policy function, at least one refinement template and at least one available policy function from the at least one memory, receives a policy input indicating a high-level policy for the IT system where the policy input is compliant with the at least one policy function and is received in a format that is not machine-enforceable at an enforcement entity of the IT system, based on the received policy input, automatically or semi-automatically generates a machine-enforceable rule and/or configuration by filling the at least one refinement template, where the machine-enforceable rule and/or configuration includes the at least one available policy function and being compliant with the received policy input, and distributes the machine-enforceable rule and/or configuration to the at least one memory of the IT system or another at least one memory to

thereby enable implementation of the policies.

8/12 © PATENW / EPO

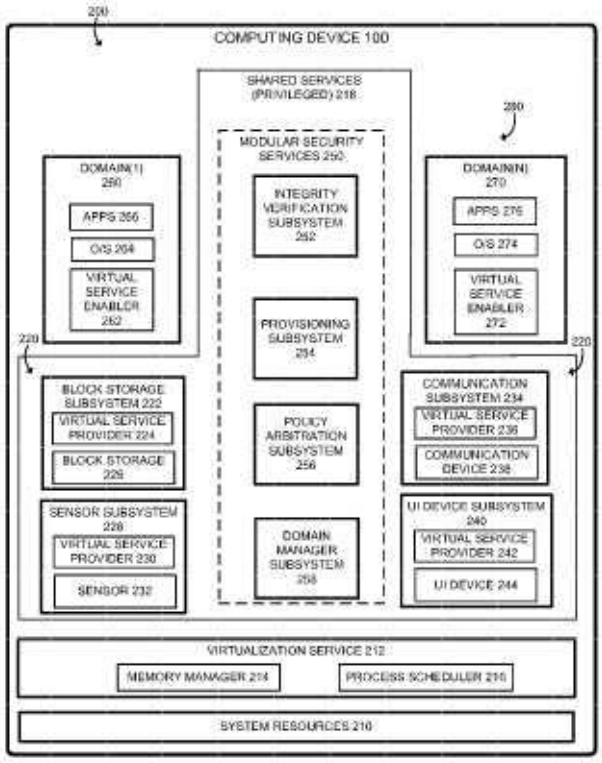
PN - US2014380425 A1 20141225

PR - US201314052266 20131011; US201361839202P 20130625; US201313872865 20130429

AP - US201314052266 20131011

DT - **

CT - || R141 (A1)
US6134594 A 20001017 [ ] (HELLAND PATRICK JAMES [US], et al);
US6256771 B1 20010703 [ ] (O'NEIL JOSEPH THOMAS [US], et al);
US6324619 B1 20011127 [ ] (RAVERDY PIERRE-GUILLAUME [US], et al);
US6854107 B2 20050208 [ ] (GREEN DAVID W [US], et al);
US2005233744 A1 20051020 [ ] (KARAOGUZ JEYHAN [US], et al);
US2007298719 A1 20071227 [ ] (SPROULE WILLIAM D [US], et al);
US2009089860 A1 20090402 [ ] (FORRESTER RONALD JAMES [US], et al);
US2009125880 A1 20090514 [ ] (MANOLESCU DRAGOS A [US], et al);
US7676608 B1 20100309 [ ] (CROSMER JULIANNE R [US], et al);
US2010319053 A1 20101216 [ ] (GHARABALLY SAM [US]);
US6643262 B1 20031104 [ ] (LARSSON TONY INGEMAR [SE], et al);
US2008114973 A1 20080515 [ ] (NORTON SCOTT J [US], et al);
US2008184274 A1 20080731 [ ] (OHTA KEN [JP], et al);
US2008318616 A1 20081225 [ ] (CHIPALKATTI RENU [US], et al);



US2011145833 A1 20110616 [ ] (DE LOS REYES GUSTAVO [US], et al);
US8204480 B1 20120619 [ ] (LINDTEIGEN TY [US], et al);
US8270963 B1 20120918 [ ] (HART STEVEN R [US], et al);
US8458800 B1 20130604 [ ] (VAN VOORHEES FRANKLIN DAVID [US], et al);
US8495731 B1 20130723 [ ] (MAR PHIL [US], et al);
US2013303146 A1 20131114 [ ] (VAN VOORHEES FRANKLIN DAVID [US], et al);
US2014115693 A1 20140424 [ ] (SCHIEMAN ADAM RICHARD [CA], et al);
US2014179271 A1 20140626 [ ] (GUCCIONE LOUIS J [US], et al);
US2014325644 A1 20141030 [ ] (OBERG SCOTT [US], et al);
US2014330990 A1 20141106 [ ] (LANG ZHONGMIN [US], et al);
US2014379923 A1 20141225 [ ] (OBERG SCOTT A [US], et al);
US2014380405 A1 20141225 [ ] (FORSBERG SEAN M [US], et al);
US2014380406 A1 20141225 [ ] (SAIDI HASSEN [US], et al);
US2015363474 A1 20151217 [ ] (FOGEL CHRISTOPHER MICHAEL [CA], et al);
US2016019104 A1 20160121 [ ] (MAJOR DANIEL JONAS [CA], et al)

- || STSE (B2)

US6134594 A 20001017 [ ] (HELLAND PATRICK JAMES [US], et al);
US6256771 B1 20010703 [ ] (O'NEIL JOSEPH THOMAS [US], et al);
US6324619 B1 20011127 [ ] (RAVERDY PIERRE-GUILLAUME [US], et al);
US6643262 B1 20031104 [ ] (LARSSON TONY INGEMAR [SE], et al);

US6854107 B2 20050208 [ ] (GREEN DAVID W [US], et al);
US7676608 B1 20100309 [ ] (CROSMER JULIANNE R [US], et al);
US8204480 B1 20120619 [ ] (LINDTEIGEN TY [US], et al);
US8270963 B1 20120918 [ ] (HART STEVEN R [US], et al);
US8458800 B1 20130604 [ ] (VAN VOORHEES FRANKLIN DAVID [US], et al);
US8495731 B1 20130723 [ ] (MAR PHIL [US], et al);
US2005233744 A1 20051020 [ ] (KARAOGUZ JEYHAN [US], et al);
US2007298719 A1 20071227 [ ] (SPROULE WILLIAM D [US], et al);
US2008114973 A1 20080515 [ ] (NORTON SCOTT J [US], et al);
US2008184274 A1 20080731 [ ] (OHTA KEN [JP], et al);
US2008318616 A1 20081225 [ ] (CHIPALKATTI RENU [US], et al);
US2009089860 A1 20090402 [ ] (FORRESTER RONALD JAMES [US], et al);
US2009125880 A1 20090514 [ ] (MANOLESCU DRAGOS A [US], et al);
US2010319053 A1 20101216 [ ] (GHARABALLY SAM [US]);
US2011145833 A1 20110616 [ ] (DE LOS REYES GUSTAVO [US], et al);
US2013303146 A1 20131114 [ ] (VAN VOORHEES FRANKLIN DAVID [US], et al);
US2014115693 A1 20140424 [ ] (SCHIEMAN ADAM RICHARD [CA], et al);
US2014179271 A1 20140626 [ ] (GUCCIONE LOUIS J [US], et al);
US2014325644 A1 20141030 [ ] (OBERG SCOTT [US], et al);
US2014330990 A1 20141106 [ ] (LANG ZHONGMIN [US], et al);
US2014379923 A1 20141225 [

] (OBERG SCOTT A [US], et al); US2014380405 A1 20141225 [ ] (FORSBERG SEAN M [US], et al); US2014380406 A1 20141225 [ ] (SAIDI HASSEN [US], et al); US2015363474 A1 20151217 [ ] (FOGEL CHRISTOPHER MICHAEL [CA], et al); US2016019104 A1 20160121 [ ] (MAJOR DANIEL JONAS [CA], et al)

CCI - G06F21/575 ; G06F21/74 ; H04L63/08 ; H04L63/20

CUI - G06F9/542

CQI - G06F21/00 ; G06F21/60

CCA - H04W12/06 ; G06F2221/2101

CUA - H04W12/08

PA - (A1 B2)
STANFORD RES INST INT [US]

TI - (A1)
POLYMORPHIC COMPUTING ARCHITECTURES
- (B2)
Polymorphic computing architectures

AB - (A1)
Polymorphic computing architectures can support and control separate, independently executable domains and other components on a computing platform. In some embodiments, the architectures may control the different domains and/or components according to different purposes. In some embodiments, the architectures can control domains and/or components to enforce a desired “purpose” of a domain/component while simultaneously denying a corresponding “anti-purpose.”
- (B2)
Polymorphic computing architectures can support and control separate, independently

executable domains and other components on a computing platform. In some embodiments, the architectures may control the different domains and/or components according to different purposes. In some embodiments, the architectures can control domains and/or components to enforce a desired "purpose" of a domain/component while simultaneously denying a corresponding "anti-purpose".

9/12 © PATENW / EPO

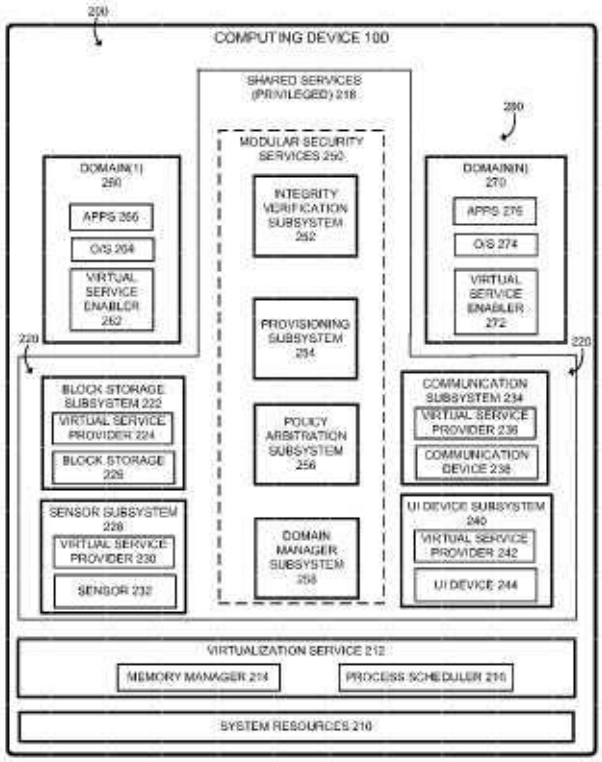
PN - US2014380405 A1 20141225

PR - US201314052080 20131011; US201361839202P 20130625; US201313872865 20130429

AP - US201314052080 20131011

DT - **

CT - || R141 (A1)
US9075955 B2 20150707 [ ] (SCHIEMAN ADAM RICHARD [CA], et al);
US7734933 B1 20100608 [ ] (MAREK JAMES A [US], et al);
US8931042 B1 20150106 [ ] (WEISS YOAV [IL]);
US2009271844 A1 20091029 [ ] (ZHANG XINWEN [US], et al);
US2013055378 A1 20130228 [ ] (CHANG YOUN-JOO [KR], et al);
US2013227641 A1 20130829 [ ] (WHITE CHRISTOPHER JULES [US], et al);
US2013263206 A1 20131003 [ ] (NEFEDOV NIKOLAI [CH], et al);
US2014280952 A1 20140918 [ ] (SHEAR VICTOR HENRY [US], et al);
US2014330990 A1 20141106 [ ] (LANG ZHONGMIN [US], et al);
US2014157351 A1 20140605 [ ] (CANNING SIMON GILBERT [AU], et al)



- || STSE (B2)
US7734933 B1 20100608 [ ] (MAREK JAMES A [US], et al);
US8931042 B1 20150106 [ ] (WEISS YOAV [IL]);
US9075955 B2 20150707 [ ] (SCHIEMAN ADAM RICHARD [CA], et al);
US2009271844 A1 20091029 [ ] (ZHANG XINWEN [US], et al);
US2013055378 A1 20130228 [ ] (CHANG YOUN-JOO [KR], et al);
US2013227641 A1 20130829 [ ] (WHITE CHRISTOPHER JULES [US], et al);
US2013263206 A1 20131003 [ ] (NEFEDOV NIKOLAI [CH], et al);
US2014157351 A1 20140605 [ ] (CANNING SIMON GILBERT [AU], et al);
US2014280952 A1 20140918 [ ] (SHEAR VICTOR HENRY [US], et al);
US2014330990 A1 20141106 [ ] (LANG ZHONGMIN [US], et al)

CCI - G06F21/575 ; G06F21/74 ; H04L63/08 ; H04L63/20

CUI - G06F9/542

CQI - G06F21/00 ; G06F21/60

CCA - H04W12/06 ; G06F2221/2101

CUA - H04W12/08

PA - (A1 B2)
STANFORD RES INST INT [US]

TI - (A1)
FLEXIBLE POLICY ARBITRATION CONTROL SUITE

- (B2)
Flexible policy arbitration control suite

AB - (A1 B2)
A policy arbitration system manages the fundamental communications and isolation between executable components and shared system resources of a computing device, and controls the use of the shared resources

by the executable components. Some versions of the policy arbitration system operate on a virtualized mobile computing device to dynamically compile and implement policy rules that are issued periodically by multiple different independent execution environments that are running on the computing device. Semi-dynamic policy changes allow for context enabled policy changes that enforce the desired system and component "purpose" while simultaneously denying the "anti-purpose".

10/12 © PATENW / EPO

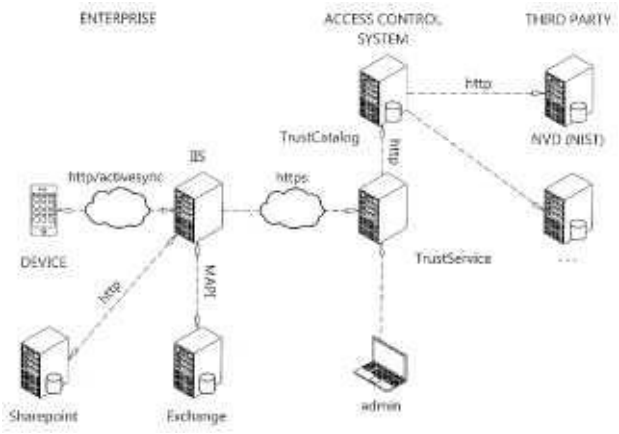
PN - US2013239167 A1 20130912

PR - US201213414531 20120307

AP - US201213414531 20120307

DT - *; Rep

CT - || R141 (A1)
US2010306827 A1 20101202 [ ] (ESTEVE BALDUCCI JUAN V [US], et al);
US2006020792 A1 20060126 [ ] (WEISS JASON R [US])
- || STSE (B2)
US8234705 B1 20120731 [ ] (ROSKIND JAMES A [US], et al);
US2006020792 A1 20060126 [ ] (WEISS JASON R [US]);
US2006191012 A1 20060824 [ ] (BANZHOF CARL E [US], et al);
US2008120699 A1 20080522 [ ] (SPEAR PAUL R [US]);
US2009077666 A1 20090319 [ ] (CHEN YUE [US], et al);
US2010057631 A1 20100304 [ ] (WARNER NEIL [US]);
US2010223670 A1 20100902 [ ] (CASTELL WILLIAM D [CA], et al);
US2010306827 A1 20101202 [ ] (ESTEVE BALDUCCI JUAN V [US], et al);
US2011119765 A1 20110519 [ ] (HERING JOHN G [US], et al)



CCI - G06F21/44 ; G06F21/577 ; H04W12/12

CCA - H04L63/1433

PA - (A1)
SREENIVAS GIRIDHAR [US]; SIGURDSON DEREK [US]

- (B2)
SREENIVAS GIRIDHAR [US]; SIGURDSON DEREK [US]; RAPID 7 INC [US]

TI - (A1)
CONTROLLING ENTERPRISE ACCESS BY MOBILE DEVICES

- (B2)
Controlling enterprise access by mobile devices

AB - (A1 B2)
A system comprising at least one component running on at least one server and receiving vulnerability data and, for each device of a plurality of devices, device data that includes data of at least one device component. The system includes a trust score corresponding to each device of the plurality of devices and representing a level of security applied to the device. The trust score is generated using a severity of the vulnerability data. The system includes an access control component coupled to the at least one component and controlling access of the plurality of devices to an enterprise using the trust score.

Do you wish to continue ? (Y/N) N

[SS 4]