



WINCC UNDER X-RAYS

Sergey Gordeychik
Denis Baranov
Gleb Gritsai

Who we are

- ▣ **Sergey Gordeychik**
 - **Positive Technologies** CTO, **Positive Hack Days** Director and Scriptwriter, WASC board member
- ▣ **Gleb Gritsai (@repdet)**
 - Principal Researcher, Network security and forensic expert, head of **PHDays Challenges** team
- ▣ **Denis Baranov**
 - Head of AppSec group, researcher, member of **PHDays Challenges** team

<http://www.phdays.com> <http://blog.ptsecurity.com>

<http://scadasl.org>

SCADAStrangeLove.org

- ▣ Group of security researchers focused on ICS/SCADA

to **save** Humanity **from** industrial **disaster** and to
keep Purity Of Essence

Sergey Gordeychik

Roman Ilin

Artem Chaykin

Dmitry Efanov

Andrey Medov

Alexander Zaitsev

Dmitry Sklyarov

Ilya Smith

Gleb Gritsai

Ilya Karpov

Yuriy Dyachenko

Yuri Goltsev

Sergey Scherbel

Dmitry Serebryannikov

Alexander Timorin

Roman Ilin

Denis Baranov

Sergey Bobrov

Sergey Drozdov

Vladimir Kochetkov

Timur Yunusov

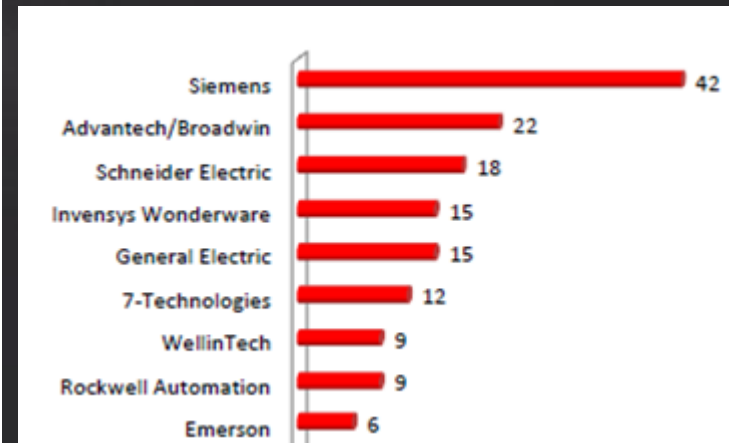
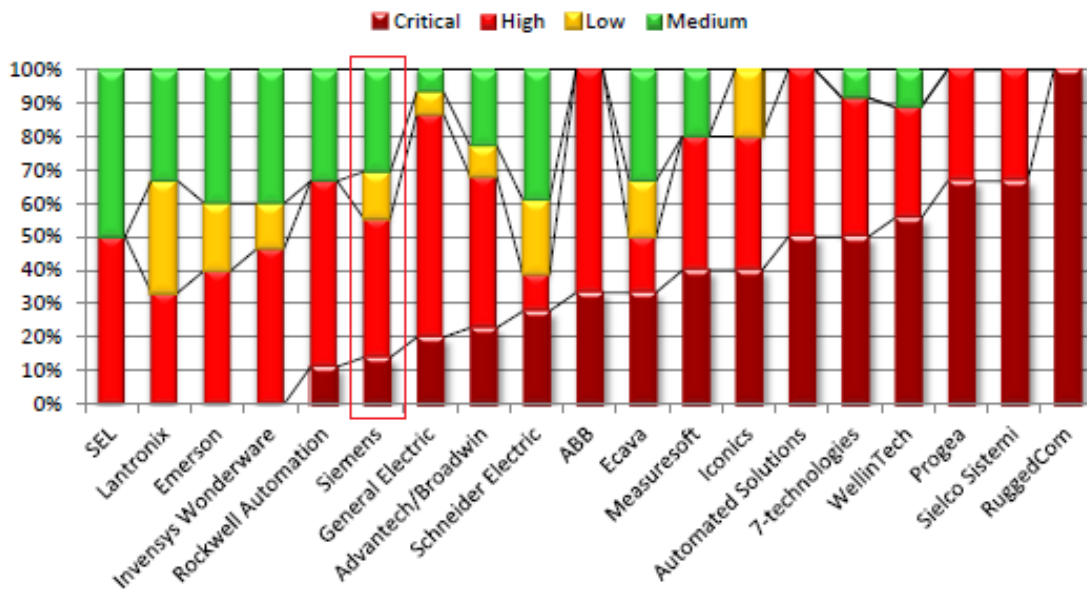
Dmitry Nagibin

Vyacheslav Egoshin

Alexander Tlyapov

Why Siemens?

- Common target during pentests
- Most common platform (market, ShodanHQ)
- Largest number of published and **fixed** bugs



Special thanks to

- ▣ Siemens ProductCERT
 - **Really** professional team
 - Quick responses
 - Patches!

- ▣ **You guys rock!**

...under X-Rays

- ▣ Invensys Wonderware
- ▣ Yokogawa
- ▣ ICONICS
- ▣

- ▣ *Stay tuned!*

Our goals

- ▣ Goals

 - to automate security assessment of ICS platforms and environment

- ▣ Objectives

 - to understand system

 - to assess built-in security features

 - to create security audit/hardening guides

 - to automate process

Vulnerabilities – waste production

Our approach









Siemens SIMATIC WinCC

WinCC Distributed Architecture

- ▣ WinCC Server
 - Windows/MSSQL based SCADA
- ▣ WinCC Client (HMI)
 - WinCC runtime + project
- ▣ WinCC Web Server (WebNavigator)
 - IIS/MSSQL/ASP/ASP.NET/SOAP
- ▣ WinCC WebClient (HMI)
 - ActiveX/HTML/JS

B-Sides and Rarities

- ▣ Big Project
- ▣ Long History
- ▣ A lot of obsolete
 - code
 - features
 - third parties
 - ...

1825-day exploit

The image shows a Windows command prompt window with the following commands and output:

```
C:\>cd "\Program Files\Siemens"  
C:\Program Files\Siemens>dir /s | findstr "\.200." | find "exe" > oldexe.txt
```

Below the command prompt is a screenshot of the SCADA WinCC AC interface. The window title is "[SCADA] WinCC AC [Started: 02.11.2012 11:23, duration 00:10:31]". The interface has a top navigation bar with "Audit", "Compliance", and "Summary/hosts" buttons. The main area is split into two panes:

- Navigator:** Shows a tree view of vulnerabilities. The "OpenSSL" folder is expanded, showing several instances of "0.9.8e". Underneath, various vulnerability types are listed, including "Arbitrary Code Execution", "Heap-Based Buffer Overflow", "Buffer Overflow", "Certificate Validation Vulnerability", "Denial of Service", "Integer Underflow", "Memory Leakage", "Security Restriction Bypass", "Security Restrictions Bypassing", "Unauthorized Access", and "Information Disclosure".
- Information:** Displays details for a high-level vulnerability. It shows a red circle icon and the text "High level Service: [OpenSSL]". Below this is a table with the following information:

Version:	0.9.8e
Detection method:	by files
Path:	C:\Program Files\Siemens\SIMATIC.NET\tools
Maximum vulnerability level:	high level
The number of vulnerabilities detected:	20

On the right side of the interface, there is a partial view of another window showing text related to "le Software", "SL 0.9.7 up", "xecute", "underflow.", "738. As of", "lp distinguish", "e buffer", and "0/0/threaded".

DiagAgent (CVE-2012-2598)

Remote management tool (FS/registry), HTTP
8080

Not started by default and shouldn't be running
ever



- ❑ No authentication at all
- ❑ XSSes
- ❑ Buffer overflow (GET /AAAAAAAA....AAAAA)

SOLUTION

Updates correcting the first three issues are now available in the Update 2 for WinCC V7.0 SP3 [1]. Siemens AG recommends applying this patch as soon as possible.

Siemens AG also recommends **not using DiagAgent anymore** since it is not supported anymore. Customers can migrate to the SIMATIC Diagnostics Tool [5] or the SIMATIC Analyser [6].

Encrypt (Server Side)

```
Function Encrypt (secret, PassWord)
```

```
    ' secret$ = the string you wish to encrypt or decrypt.
```

```
    ' PassWord$ = the password with which to encrypt the string.
```

```
    dim L, X, s, Char
```

```
    L = Len(PassWord)
```

```
    For X = 1 To Len(secret)
```

```
        Char = Asc(Mid(PassWord, (X Mod L) - L * ((X Mod L) = 0),  
1))
```

```
        'Mid(secret, X, 1) = Chr(Asc(Mid(secret, X, 1)) Xor Char)
```

```
        s = s & Chr(Asc(Mid(secret, X, 1)) Xor Char)
```

```
    Next
```

```
    Encrypt = Escape(s)
```

```
End Function
```

Decrypt (Client Side)

Function Decrypt (secret, PassWord)

' secret\$ = the string you wish to encrypt or decrypt.

' PassWord\$ = the password with which to encrypt the string.

dim L, X, s, Char

secret = Unescape(secret)

L = Len(PassWord)

For X = 1 To Len(secret)

Char = Asc(Mid(PassWord, (X Mod L) - L * ((X Mod L) = 0), 1))

'Mid(secret, X, 1) = Chr(Asc(Mid(secret, X, 1)) Xor Char)

s = s & Chr(Asc(Mid(secret, X, 1)) Xor Char)

Next

Decrypt = s

End Function

Encrypt vs Decrypt

Function **EnDecrypt** (secret, PassWord)

' secret\$ = the string you wish to encrypt or decrypt.

' PassWord\$ = the password with which to encrypt the string.

dim L, X, s, Char

secret = Unescape(secret)

L = Len(PassWord)

For X = 1 To Len(secret)

Char = Asc(Mid(PassWord, (X Mod L) - L * ((X Mod L) = 0), 1))

'Mid(secret, X, 1) = Chr(Asc(Mid(secret, X, 1)) Xor Char)

s = s & Chr(Asc(Mid(secret, X, 1)) Xor Char)

Next

Encrypt = Escape(s)

Decrypt = s

End Function

Fighting with

To analyze:

- Files not changed for a while
- Third-party tools and libraries

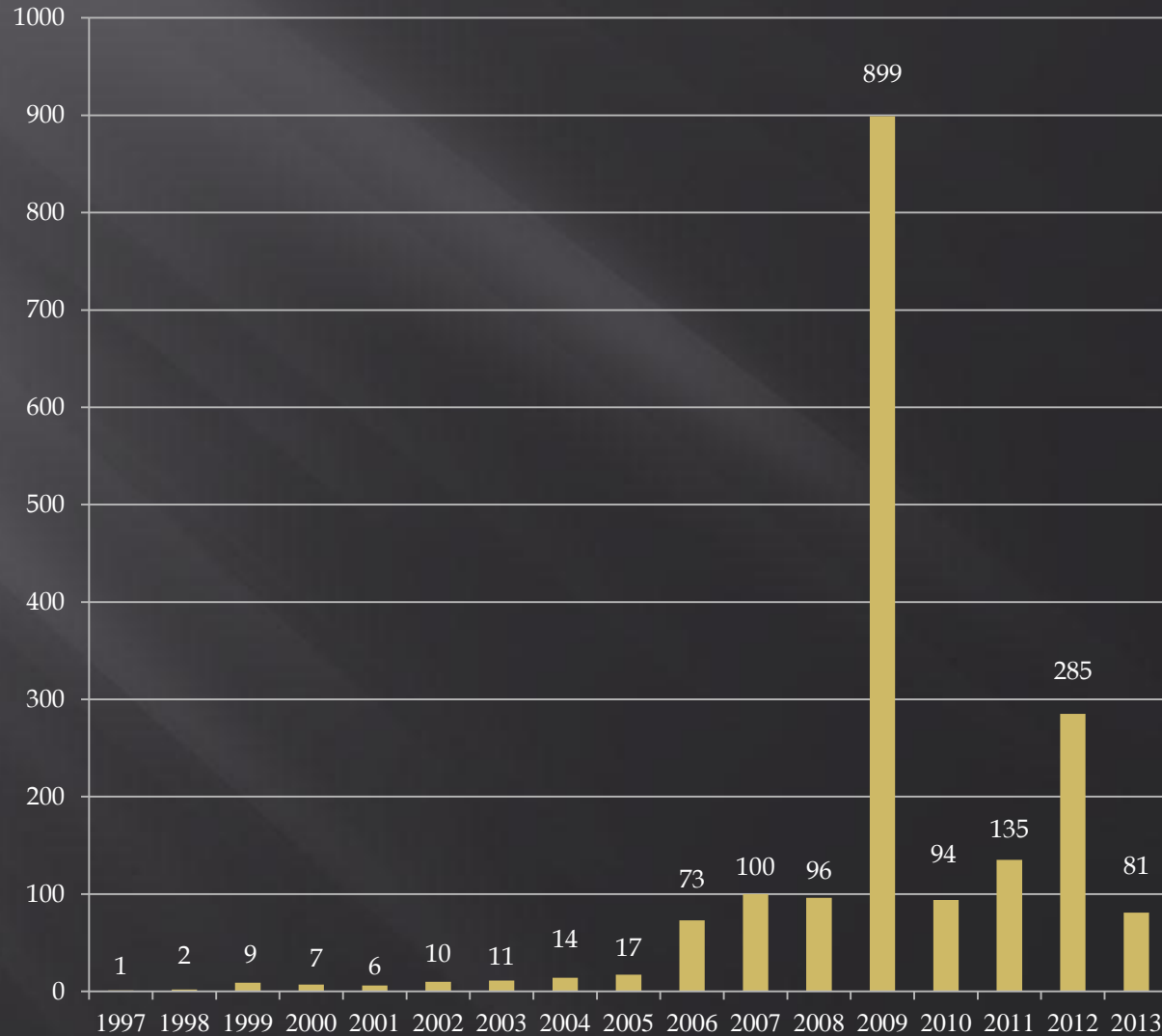
To automate:

- Control of change/commit dates
- Host-level scanners/fingerprint tools

Processes:

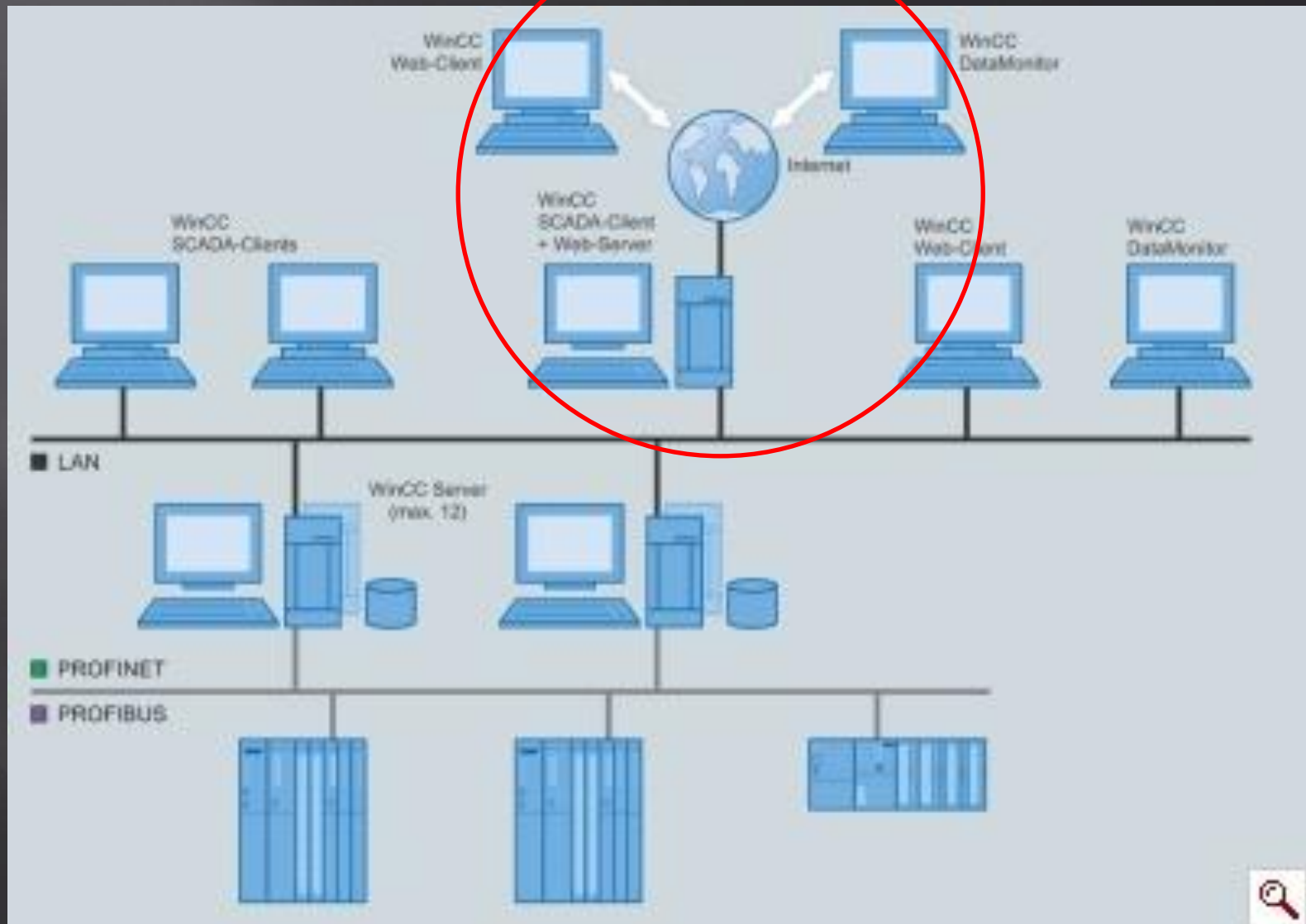
- **Know your third-party!**

Know your third-party



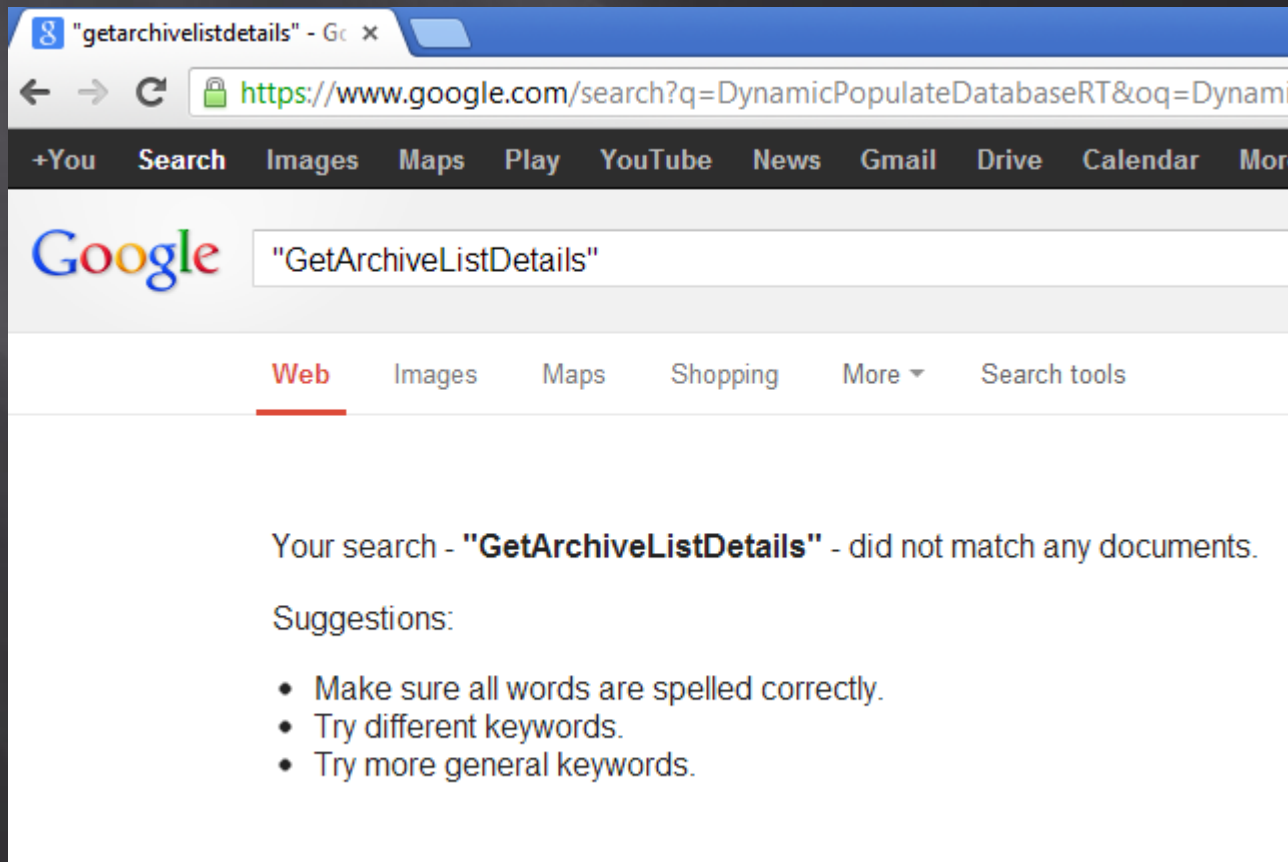
CompanyName	Adobe Systems Incorporated
CompanyName	Blue Sky Software
CompanyName	ClassWorks
CompanyName	Datalogics, Inc.
CompanyName	Free Software Foundation
CompanyName	IBM Corporation and others
CompanyName	InstallShield Software Corporation
CompanyName	Microsoft Corporation
CompanyName	OPC Foundation
CompanyName	Rogue Wave Software
CompanyName	Stingray Software Inc.
CompanyName	SynCFusion Inc.
CompanyName	The OpenSSL Project,
CompanyName	VisualTools Inc.
CompanyName	WexTech Systems, Inc.

WebNavigator



AutoComplete SOAP interface

- ▣ Available at /WebCenter/AutoComplete.asmx
- ▣ Well-documented



AutoComplete SOAP interface

- ▣ Available at /WebCenter/AutoComplete.asmx
- ▣ Well Self-documented

The following operations are supported. For more information, click on the operation name.

- [DynamicPopulateDatabaseRT](#)
- [GetArchiveListDetails](#)
- [GetCompetitionItemsForArchiveView](#)
- [GetHelpContext](#)
- [GetLicenseInfo](#)
- [GetProcessScreenList](#)
- [GetTagVariablenList](#)

AutoComplete

Click [here](#) for a complete list of operations.

GETARCHIVELISTDETAILS

Test

The test form is only available for requests from the local machine.

SOAP 1.1

The following is a sample SOAP 1.1 request and response. The **placeholders** shown need to be replaced with actual values.

```
POST /WebCenter/AutoComplete.asmx HTTP/1.1
Host: hostname
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "Siemens.Simatic.WinCC.DataMonitor/GetArchiveListDetails"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <GetArchiveListDetails xmlns="Siemens.Simatic.WinCC.DataMonitor">
      <contextKey>string</contextKey>
    </GetArchiveListDetails>
  </soap:Body>
</soap:Envelope>
```

Not so well self documented

- ▣ Undocumented method

Siemens.Simatic.WinCC.DataMonitor

/GetServerList

Live HTTP Replay

POST http://192.168.1.100:8080/WebCenter/AutoComplete.asmx HTTP/1.1

HTTP Headers

Host: 192.168.1.100
Host: 192.168.1.100
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "Siemens.Simatic.WinCC.DataMonitor/GetServerList"
Authorization: Basic [REDACTED]

POST ?

```
<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <GetServerList xmlns="Siemens.Simatic.WinCC.DataMonitor">
      <prefixText></prefixText>
      <count>9</count>
    </GetServerList>
  </soap:Body>
</soap:Envelope>
```

Content-Length: 384

Повтор Закреть

But useful

```
<soap:Envelope>
- <soap:Body>
  - <GetServerListResponse>
    - <GetServerListResult>
      - <string>
        {"First":"STANDWINCC7 (WINCC)","Second":"STANDWINCC7WINCC"}
      </string>
      - <string>
        {"First":"COMPUTER-D22053 (WINCCPLUSMIG)","Second":"COMPUTER-D22053WINCCPLUSMIG"}
      </string>
      - <string>
        {"First":"COMPUTER-D22053 (WINCC)","Second":"COMPUTER-D22053WINCC"}
      </string>
      - <string>
        {"First":"KDA-34B1DA5A033 (WINCC)","Second":"KDA-34B1DA5A033WINCC"}
      </string>
```

- ▣ SQL Servers in subnet enumeration
- ▣ SQL-type Injection

Code review

```
    alert(Html2Xml(oNode)),
    oxml.loadXML("<NODES>" + oNode.innerHTML + "</NODES>");
    alert(oxml.xml);
    return oxml.transformNode(strPattern);
}

// dreckige Hackerei
function Html2Xml(oNode) {
    // copy the attributes first
    var attb;
    var str = new String;
    str = "<" + oNode.tagName;
    for(attb in oNode.attributes)
    {
        var attbval = oNode.getAttribute(attb);
        if(attbval != null && attbval != "")
        {
            str += " \"" + attb.nodeName + "\"=\"" + oNode.nodeValue + "\" ";
        }
    }
}
```

```
// dreckige Hackerei
function Html2Xml(oNode) {
```

WebNavigator (round 1)

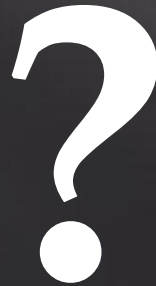
- ▣ XPath Injection (CVE-2012-2596)
- ▣ Path Traversal (CVE-2012-2597)
- ▣ XSS ~ 20 Instances (CVE-2012-2595)

Fixed in Update 2 for WinCC V7.0 SP3

<http://support.automation.siemens.com/WW/view/en/60984587>

XSS in HMI? So what?

- ▣ Can help to exploit server-side vulnerabilities
- ▣ Operator's browser is proxy to SCADAnet!







- ▣ Anybody works with SCADA and Internet using same browser?

Client-side WinCC Fingerprint

SP SURFPATROL Русский About SurfPatrol Help Forum Login

Home

SurfPatrol has checked your browser and its plug-ins. Detected vulnerabilities: 3

	Internet Explorer 9.0.8112.16421	Open recommendations
	Adobe Reader Plugin 10.1.0	Open recommendations
	Siemens SIMATIC WinCC HMI ActiveX Control 700.2100.151.3 It is unsafe to use industrial control workstations for web browsing. Vulnerabilities in SCADA systems, which can be exploited by malicious people to conduct cross-site scripting attacks, disclose potentially sensitive information, cause a DoS (Denial of Service), and compromise a vulnerable system. Additional information	Hide recommendations
	Java Runtime 1.7.0.10	No flaws detected

<http://www.surfpatrol.ru/en/report>

You should never underestimate
the predictability of ...

- ▣ A lot of “WinCCed” IE from
countries/companies/industries
- ▣ Special prize to guys from US for
WinCC 6.X at 2012

WebNavigator (round 2)

- ▣ Lot of XSS and CSRF
 - CVE-2012-3031
 - CVE-2012-3028
- ▣ Lot of arbitrary file reading
 - CVE-2012-3030
- ▣ SQL injection over SOAP
 - CVE-2012-3032
- ▣ Username and password disclosure via **ActiveX** abuse
 - CVE-2012-3034

Fixed in Update 3 for WinCC V7.0 SP3

<http://support.automation.siemens.com/WW/view/en/63472422>

Fun with ActiveX

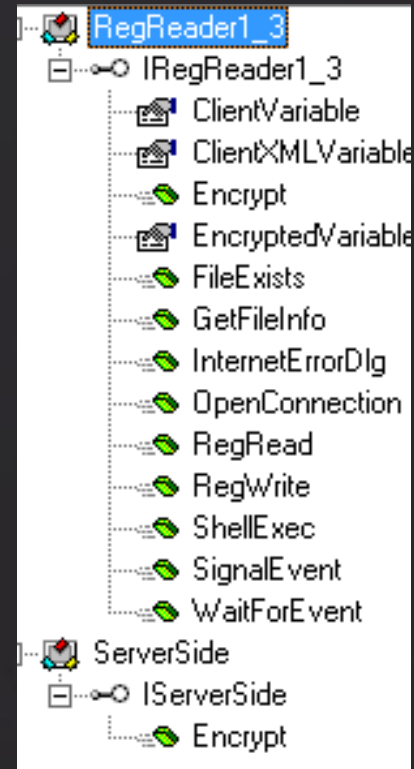
- ▣ Interesting objects and methods

WebClientInstall.RegReader.RegRead

IsAdministrator()

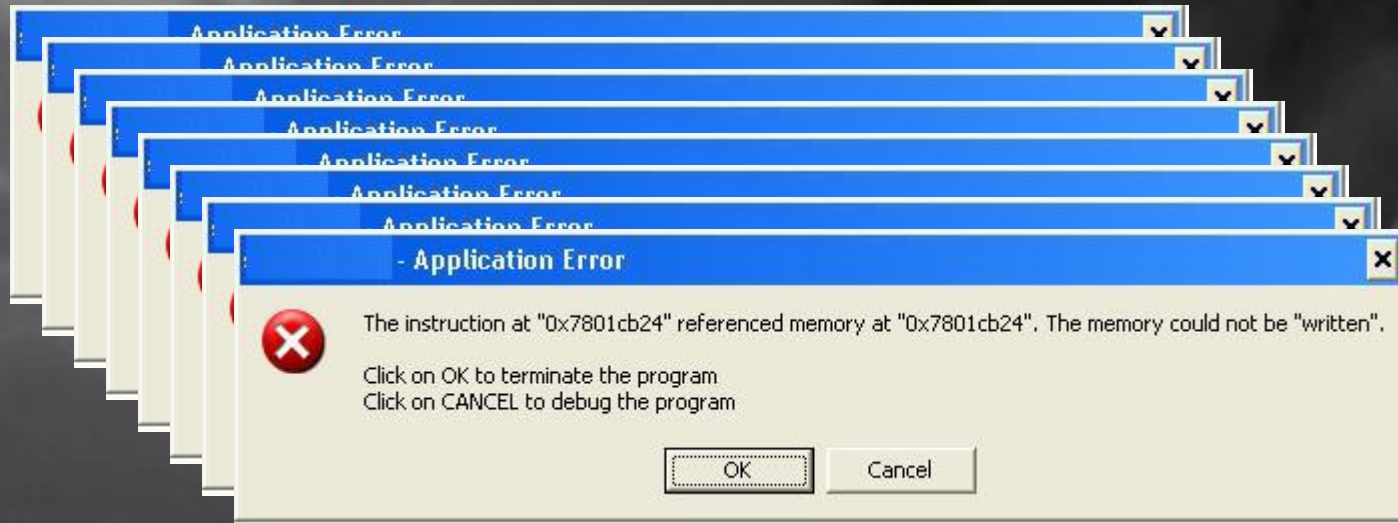
IsPowerUser()

openConnection()



- ▣ Can't use ShellExecute of something...
- ▣ Restricted but still exists for compatibility

ComRaider still rocks!



CVE-2012-3034

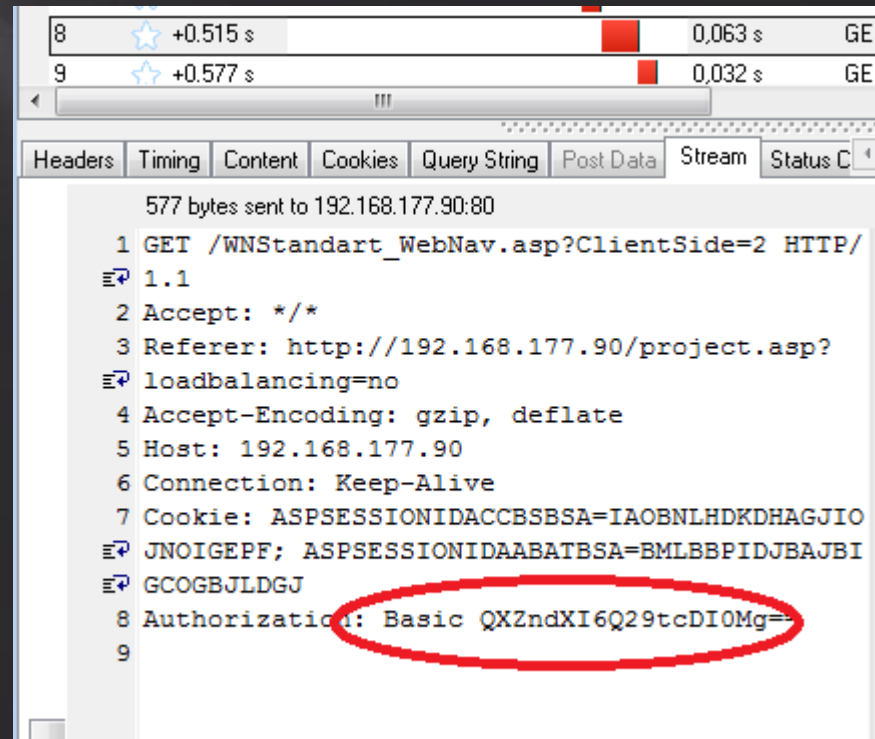
- ▣ WinCCViewer ActiveX store credentials in innerHTML
- ▣ We can get it via XSS

Demo



It fixed, but...

- ▣ How this ActiveX gets Basic account plaintext?
- ▣ How to get Authorization header on Client?
- ▣ Why ActiveX need password?
- ▣ Lets check...



The screenshot shows a web browser's developer tools window. The 'Headers' tab is selected, displaying the request headers for an HTTP GET request. The headers are as follows:

```
577 bytes sent to 192.168.177.90:80
1 GET /WNStandart_WebNav.asp?ClientSide=2 HTTP/1.1
2 Accept: */*
3 Referer: http://192.168.177.90/project.asp?loadbalancing=no
4 Accept-Encoding: gzip, deflate
5 Host: 192.168.177.90
6 Connection: Keep-Alive
7 Cookie: ASPSESSIONIDACCBSBSA=IAOBNLHDKDHAGJIOJNOIGEPF; ASPSESSIONIDAABATBSA=BMLBBPIDJBAJBIGCOGBJLDGJ
8 Authorization: Basic QXZndXI6Q29tcDI0Mg==
9
```

The 'Authorization: Basic QXZndXI6Q29tcDI0Mg==' header is circled in red, indicating the plaintext password being sent in the request.

NO. [Dropdown] OffSet Timeline Duration(s) Method Result Receive

00:00:00.000 CCEClient.exe[5944] (Count=3, Sent=1,51 K, Received=0, ElapsedTime=4,415 s)

NO.	Offset	Duration(s)	Method
1	+0.000 s	0,251 s	POST
2	+3.339 s	0,234 s	POST
3	+4.165 s	0,250 s	POST

NO.	Offset	Duration(s)	Method
8	+0.515 s	0,063 s	GET
9	+0.577 s	0,032 s	GET

Headers Timing Content Cookies Query String Post Data Stream Status C

504 bytes sent to 192.168.177.90:80

```
1 POST /SCSWebBridge/SCSWebBridgeX.dll?ID=65537 HTTP/1.1
2 Cache-Control: no-cache
3 Connection: Keep-Alive
4 Pragma: no-cache
5 User-Agent: SCSPALClient
6 Content-Length: 219
7 Host: 192.168.177.90
8 Authorization: Basic V05VU1JfREM5MkQ3MTc5RTI5OkMxMDMyMzZDRThEOTg2ODhFNDgyMEQ4NTQ5NjIwNjc0
```

Headers Timing Content Cookies Query String Post Data Stream Status C

577 bytes sent to 192.168.177.90:80

```
1 GET /WNStandart_WebNav.asp?ClientSide=2 HTTP/1.1
2 Accept: */*
3 Referer: http://192.168.177.90/project.asp?loadbalancing=no
4 Accept-Encoding: gzip, deflate
5 Host: 192.168.177.90
6 Connection: Keep-Alive
7 Cookie: ASPSESSIONIDACCBSBSA=IAOBNLHDKDHAGJIOJNOIGEPF; ASPSESSIONIDAABATBSA=BMLBBPIDJBAJBIGCOGBJLDGJ
8 Authorization: Basic QXZndXI6Q29tcDI0Mg==
```

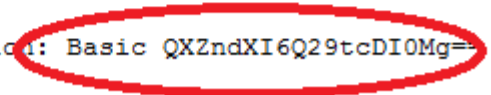
Headers Timing Content Cookies Query String Post Data Stream Status C

504 bytes sent to 192.168.177.90:80

```
1 POST /SCSWebBridge/SCSWebBridgeX.dll?ID=65537 HTTP/1.1
```

```
2 Cache-Control: no-cache
3 Connection: Keep-Alive
4 Pragma: no-cache
5 User-Agent: SCSPALClient
6 Content-Length: 219
7 Host: 192.168.177.90
8 Authorization: Basic V05VU1JfREM5MkQ3MTc5RTI5OkMxMDMyMzZDRThEOTg2ODhFNDgyMEQ4NTQ5NjIwNjc0
```

Hex View: X' < f' a' f' e x - | E • H ↓ \$ K f " K T 3 J I ↓ |



C103236CE8D98688E4820D8549620674??!



Not my ~~department~~ password!

Lets try again

```
http://[REDACTED]  
xml version="1.0" standalone="yes" ?>  
ServerData>  
<Version>K07.00.21.03_01.07.00.03</Version>  
<FileDate>Nov 23 2011</FileDate>  
<ServerID>CpxoHfRatUFe90RZe1q/pJKPXC65//U9CrtiVoI8SnPGMrD4EI0RgA ==</ServerID>  
<ConnectionSummary>  
  <Clients>0</Clients>  
  <DiagnoseClients>0</DiagnoseClients>
```

Oh! $En/c(r)ypt[10]n!$

Resume

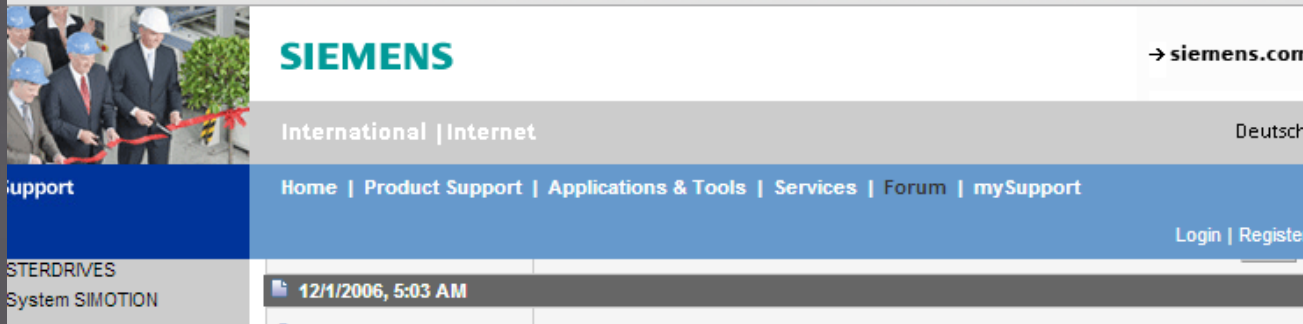
- ▣ ActiveX use hardcoded account to communicate with OPC Web bridge
- ▣ Password for WNUSR_DC92D7179E29 generated during installation and probably strong
- ▣ ~~Encrypted~~ password for WNUSR_DC* can be obtained by request to WebBridge
- ▣ But WHY?

We don't know yet



Just for history

www.automation.siemens.com/WW/forum/guests/PostShow.aspx?PageIndex=1&PostID=25933&Language=



SIEMENS → siemens.com

International | Internet Deutsch

Home | Product Support | Applications & Tools | Services | Forum | mySupport Login | Register

12/1/2006, 5:03 AM

=== Edited by Dec @ 12/1/2006 6:58 AM [GMT] ===

mentation / Analytics /
settings.



applications also.
I would like to logon on the Web Site based on Integrated Windows
Authentication regardless if I access WebNavigator or other parts of the

WebNavigator ISAPI filter WebFilter.dll uses a surrogate Account
WNUSR_DC92D7179E29 (big security flaw in my opinion because the
password is fixed and easy to find) to impersonate Windows and uses the

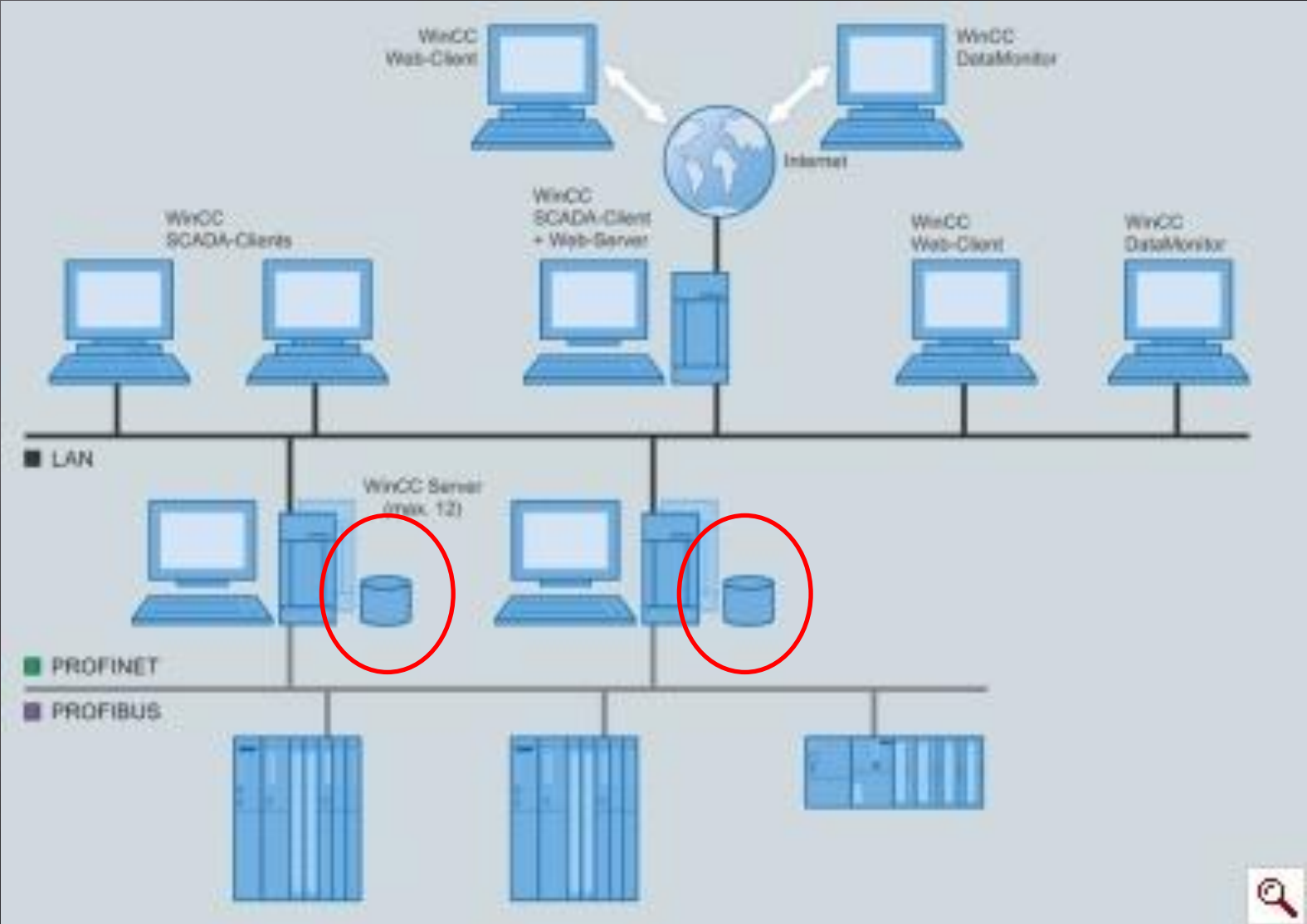


I can see "fixing" this behavior by building a higher ISAPI filter but I am not
done yet with the debugging 😊

Dec

=== Edited by Dec @ 12/1/2006 6:58 AM [GMT] ===

Database



WinCC – Database Security

- Hardcoded accounts (**fixed**)
- MS SQL listening network from the box*
 - “Security controller” restricts to Subnet
- Two-tier architecture with Windows integrated auth and direct data access
 - We don't know how to make it secure

WinCC – Hardcoded SQL*


- First noticed in **May 2005**
- Published in **April 2008**
- Abused by StuxNet in **2010**
- Fixed by Siemens in Nov **2010****
- Still **works** almost **everywhere**


*Just for history

**WinCC V7.0 SP2 Update 1



SIEMENS

Пользователь WinCCConnect

 [новая тема](#)

 [ответить](#)

Список форумов SIEMENS, Россия. IA&DT -> Системы SI

Автор	
<p>Макс Прилепский Известный Писатель</p> <p>Зарегистрирован: 14.01.2005 Сообщения: 148 Откуда: Новокузнецк</p>	<p>Добавлено Вт Май 03, 2005 1:42 Заголовок сообщения: Пользователь W</p> <p>Найден пароль для этого интегрированного пользователя БД WinCC</p>
<p>Вернуться к началу</p>	<p> профиль  лс</p>
<p>Cyber Новый писатель</p> <p>Зарегистрирован 22.10.2007 Сообщения: 14</p>	<p>Добавлено Пт Апр 11, 2008 19:27 Заголовок сообщения:</p> <p><code>login='WinCCConnect' password='2WSXcder' login='WinCCAdmin' password='2WSXcde.'</code></p>

WinCC Database

- {Hostname}_ {Project}_TLG*
 - TAG data
- CC_ {Project}_ {Timestamp}*
 - Project data and configuration
 - Users, PLCs, Privileges

Dynamic SQL in stored procedures

CC_Test_1_12_05_15_13_58_57R

- Database Diagrams
- Tables
- Views
- Synonyms
- Programmability
 - Stored Procedures
 - System Stored Procedures
 - dbo.CC_SP_AlghitList
 - dbo.CC_SP_AlghitList_Dro
 - dbo.CC_sp_PrepareHitlistT
 - dbo.CC_SP_ReadTags
 - dbo.CCAlgCreateViews
 - dbo.CCTlgCreateViews
 - dbo.sp_ccalg_ClearDataLis
 - dbo.sp_CCAlg_CreateTem
 - dbo.sp_ccalg_GetMaxCour
 - dbo.sp_ccalg_PrepareData
 - dbo.sp_ccalg_PrepareTrac
 - dbo.sp_ccalg_ReadAlgByS
 - dbo.sp_ccalg_ReadData
 - dbo.sp_ccalg_ReadDataAM
 - dbo.sp_ccalg_ReadDataLis
 - dbo.sp_CCAlgCheckV11
 - dbo.sp_CCAlgConvertQue
 - dbo.sp_CCAlgConvertQue
 - dbo.sp_cctlg_GetCompres

```
CREATE PROCEDURE [dbo].[CCAlgCreateViews] ( @ViewName sysname )
AS
BEGIN
DECLARE @Typ smallint
DECLARE @Type smallint
SELECT @Type = 0

SELECT @Typ=1
DECLARE @SQL varchar(8000)
SELECT @SQL = 'DROP VIEW '+@ViewName

IF exists (SELECT name FROM sysobjects WHERE name = @ViewName )
EXEC @SQL

DECLARE @ArchiveCount int
DECLARE @DSN varchar(128)

SELECT @SQL = 'CREATE VIEW '+@ViewName+' AS ' + CHAR(13) + CHAR(10)

DECLARE AMT_Cursor CURSOR FOR SELECT DSN FROM AMT Where Type =@T

OPEN AMT_Cursor
FETCH NEXT FROM AMT_Cursor into @DSN
SELECT @ArchiveCount = 0
```

Dynamic SQL in stored procedures

- ▣ Other procedures with SQLi
 - [dbo].[sp_CCAlg_CreateTempTable]
 - [dbo].[sp_ccalg_PrepareDataList]
 - [dbo].[sp_ccalg_PrepareTraceDataList]
 - [dbo].[sp_ccalg_ReadAlgBySchema]
 - [dbo].[sp_ccalg_ReadData]
 - [dbo].[sp_ccalg_ReadDataAMTPreselect]
- ▣ No way to exploit
- ▣ Or we don't know
- ▣ Yet

WinCC accounts

- Managed by PASSCS.EXE
- Stored in dbo.PW_USER

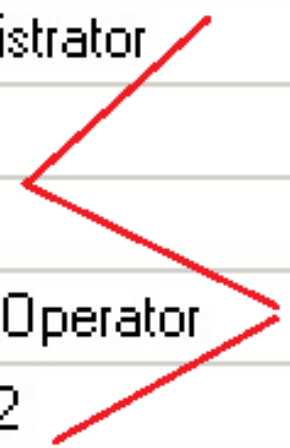
```
select ID, NAME, PASS, CAST(PASS as varbinary) from dbo.PW_USER
```

Results Messages

ID	NAME	PASS	(No column name)
10	Administrator	0.'>k&a0rq:c7 8\$;	0x142E273E6826613072713A636F372038243B3B202020202...
11	Avgur	0<'1&>p_M0	0x143C2D2231263E705F4D12202020202020202020202...
12	Admin	0.'>kot(ds0w)WGO	0x142E273E686F7428647311575D57474F2020202020202...
13	LogonOperator	0%-8_0Q 0r"<	0x19252D385F1410510A0E742A3C20202020202020202...
14	Avgur2	0<'w]0o 0Q\	0x143C2D22775D306F202912515C20202020202020202...

One!

NAME	(No column name)
Administrator	0x142E273E6B26613072713A636F372038243B3B2020:
Avgur	0x143C2D2231263E705F4D12202020202020202020:
Admin	0x142E273E6B6F7428647311575D57474F2020202020:
LogonOperator	0x19252D385F1410510A0E742A3C2020202020202020:
Avgur2	0x143C2D22775D306F202912515C2020202020202020:



Three!

```
add     eax, [ebp+var_10]
movsx   ecx, byte ptr off_463DFC      dd offset aThisIsMyEncryp ; DATA XREF: sub_4478C0+2C0↑r
mov     edx, [ebp+v                    ; sub_447CE0+11B↑r
movzx   eax, [ebp+e                    ; "This is my encryptionkey"
xor     ecx, eax
```

```
; DATA XREF: sub_4478C0+2C0↑r
sub_447CE0+11B↑r
"This is my encryptionkey"
```



**THEY KNOW
MY ENCRYPTIONKEY!**

SELECTable by

test Properties

General Member Of Profile

Member of:

- SIMATIC HMI VIEWER
- Users

Changes to a user are not effective until the next time the user logs on.

Add... Remove

OK Cancel Apply Help

SERVER\WINCC...QLQuery1.sql* Object Explorer Details

```
SELECT SYSTEM_USER
```

```
SELECT * FROM [CC_Test_1_12_12_02_22_04_37].[dbo].[PW_USER]
```

Results Messages

(No column name)

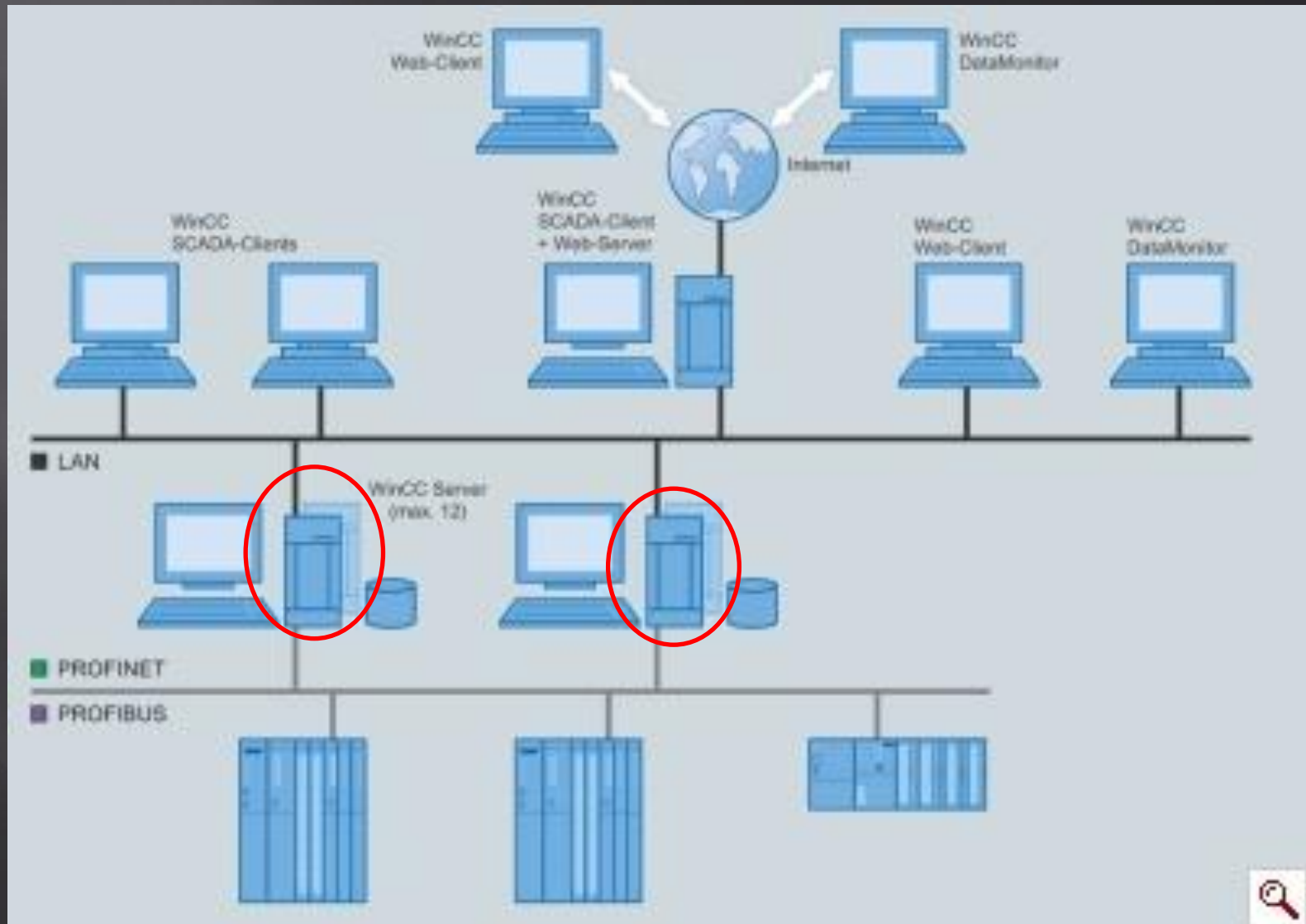
1 SERVER\test

	ID	NAME	PASS	GRPID	EXPTIME	WEBSTARTPICTURE	WEBS
1	10	Administrator	!>k&a0rq;co7 8\$;	1000	1024		1033
2	11	Avgur	!<-'1&>p_M!	1000	1024	Main.Pd_	1033
3	12	Admin	!>kot(ds!w)wGO	1000	1024		1033
4	13	LogonOperator	!%-8_!Q !*<	1001	1024		1033
5	14	Avgur2	!<-'w)Oo !Q\	1000	1024	Main.Pd_	1033

Database permissions

- ▣ Some restrictions for SQL roles
 - OPENROWSET
 - Extended Stored Procedures
 - SQL Agent functions
 - ...
- ▣ Not enough for distributed architecture
 - High privileged account for proxy is used

System Architecture



Basic objects and comms

- ▣ PdlRt.exe – graphic runtime
- ▣ CCRtsLoader.EXE – loader
- ▣ s7otbxsx.exe – network

- ▣ Inter process communication:
 - RPC
 - Sections (memory mapped files)

- ▣ \BaseNamedObjects\TCPSharedMm and other interesting stuff

Basic forensic algorithm

- ▣ Detecting active project:
HKCU\Software\SIEMENS\WINCC\Control
Center\Default Settings
 - *LastOpenPath*
 - *LastProject*
- ▣ Detecting MS SQL database name (timestamp)
 - \ *ArchiveManager\AlarmLogging*
 - \ *ArchiveManager\TagLogging**

Obtaining information from database and system
objects

The Project

- ▣ What is Project?
 - Collection of ActiveX/COM/.NET objects
 - Event Handlers and other code (C/VB)
 - Configuration files, XML and other

- ▣ Can Project be trusted?

- ▣ Ways to spread malware via Project?

Can Project be trusted?

▣ NO!

- Project itself is dynamic code
- It's easy to patch it "on the fly"
- Vulnerabilities in data handlers

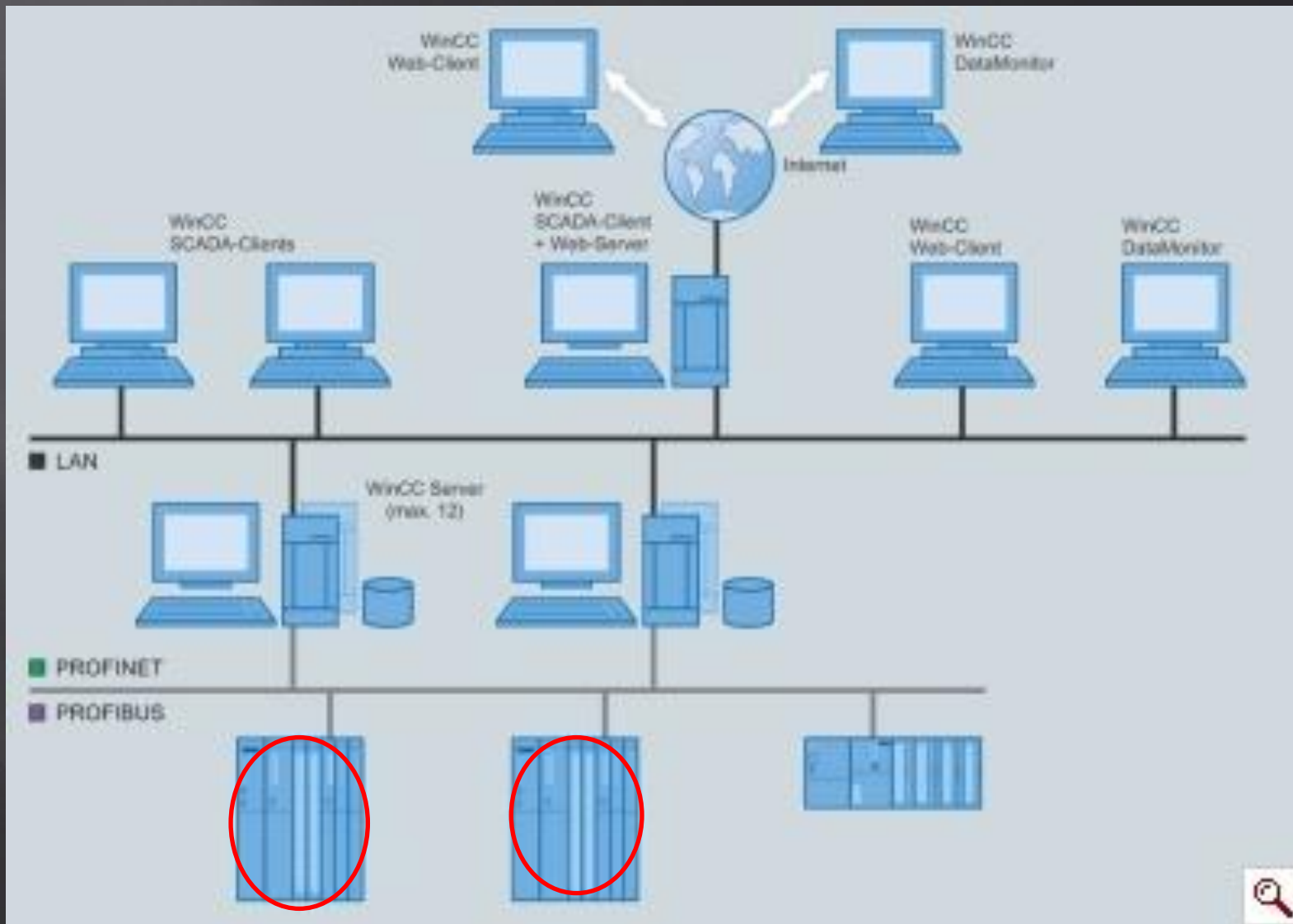
▣ How to abuse?

- Simplest way – to patch event handlers

Examples?



S7 PLC



Siemens S7 1200 PLC

- ▣ Firmware is in Intel HEX format
- ▣ Several LZSS blobs and ARM code
- ▣ Blobs contain file system for PLC
- ▣ Web application source code

... And ...

Siemens S7 PLC

- ▣ ASCII armored certificate!
- ▣ For what?
- ▣ For built-in Certification Authority

?!?!??!!!!??!

- ▣ Is there a private key?

We don't know yet



Vulnerabilities

- ▣ Hardcoded S7 PLC CA certificate (Dmitry Sklarov)

<http://scadastrangelove.blogspot.com/2012/09/all-your-plc-belong-to-us.html>

- ▣ Multiple vulnerabilities in S7 1200 PLC Web interface (Dmitriy Serebryannikov, Artem Chaikin, Yury Goltsev, Timur Yunusov)

http://www.siemens.com/corporatetechnology/pool/de/forschungsfelder/siemens_security_advisory_ssa-279823.pdf

Additional info

- ▣ MiniWeb WebServer and MWSL scripting languages (similar to WinCC Flexible)
- ▣ Ability to create and upload your own Web-pages
- ▣ InterNiche TCP/IP stack

S7 protocol

- ▣ Can be protected by password
- ▣ Authentication – simple challenge-response
 - Password hashed (SHA1) on client (TIA Portal)
 - Server (PLC) provide 20 byte challenge
 - Client calculate HMAC-SHA1(challenge, SHA1(password)) as response

Demo



Resume

- ▣ Hardcore mix of Windows and Custom Authentication/ Access Control
- ▣ Weak cryptography
- ▣ No AppSec at all (before us Siemens PCERT)
- ▣ Project is not trusted
- ▣ Some weakness in system-level design – no quick patches

Special S4x13 releases

- ▣ TIA portal Security Hardening Guide
- ▣ S7 protocol password brute force tool
- ▣ WinCC Forensic checklist

<http://scadastrangelove.blogspot.com/search/label/Releases>

Other releases

- ▣ Simatic WinCC Security Hardening Guide

<http://scadastrangelove.blogspot.com/2012/12/siemens-simatic-wincc-7x-security.html>

- ▣ PLCScan tool

<http://scadastrangelove.blogspot.com/2012/11/plcscan.html>

- ▣ ICS/SCADA/PLC Google/Shodan Cheat Sheet

<http://scadastrangelove.blogspot.com/2012/12/icsscada-plc-google-shodan-hq-cheat-sheet.html>

2 DO

- ▣ New Siemens products (TIA Portal and 1500 PLC family)
- ▣ S7 protocol vivisection
- ▣ OPC/distributed architecture protocol analysis



SCADA UNDER X-RAYS

All pictures are taken from
Engineer Garin movie and Google

SCADASTRANGELOVE.ORG