

# SCADA STRANGE LOVE OR: HOW I LEARNED TO START WORRYING AND LOVE NUCLEAR PLANTS

**Sergey Gordeychik**

**Denis Baranov**

**Gleb Gritsai**

# Who we are

- ▣ Sergey Gordeychik
  - **Positive Technologies** CTO, **Positive Hack Days** Director and Scriptwriter, WASC board member
  - <http://sgordey.blogspot.com>, <http://www.phdays.com>
- ▣ Gleb Gritsai
  - Principal Researcher, Network security and forensic researcher, member of **PHDays Challenges** team
  - @repdet, <http://repdet.blogspot.com>
- ▣ Denis Baranov
  - Head of AppSec group, researcher, member of **PHDays CTF** team

# SCADAStrangeLove.org

- ▣ Group of security researchers focused on ICS/SCADA

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

Denis Baranov

Sergey Bobrov

Artem Chaykin

Yuriy Dyachenko

Sergey Drozdov

Dmitry Efanov

Gleb Gritsai

Yuri Goltsev

Sergey Gordeychik

Roman Ilin

Vladimir Kochetkov

Andrey Medov

Sergey Scherbel

Timur Yunusov

Alexander Zaitsev

Dmitry Serebryannikov

Dmitry Nagibin

# Special thanks to

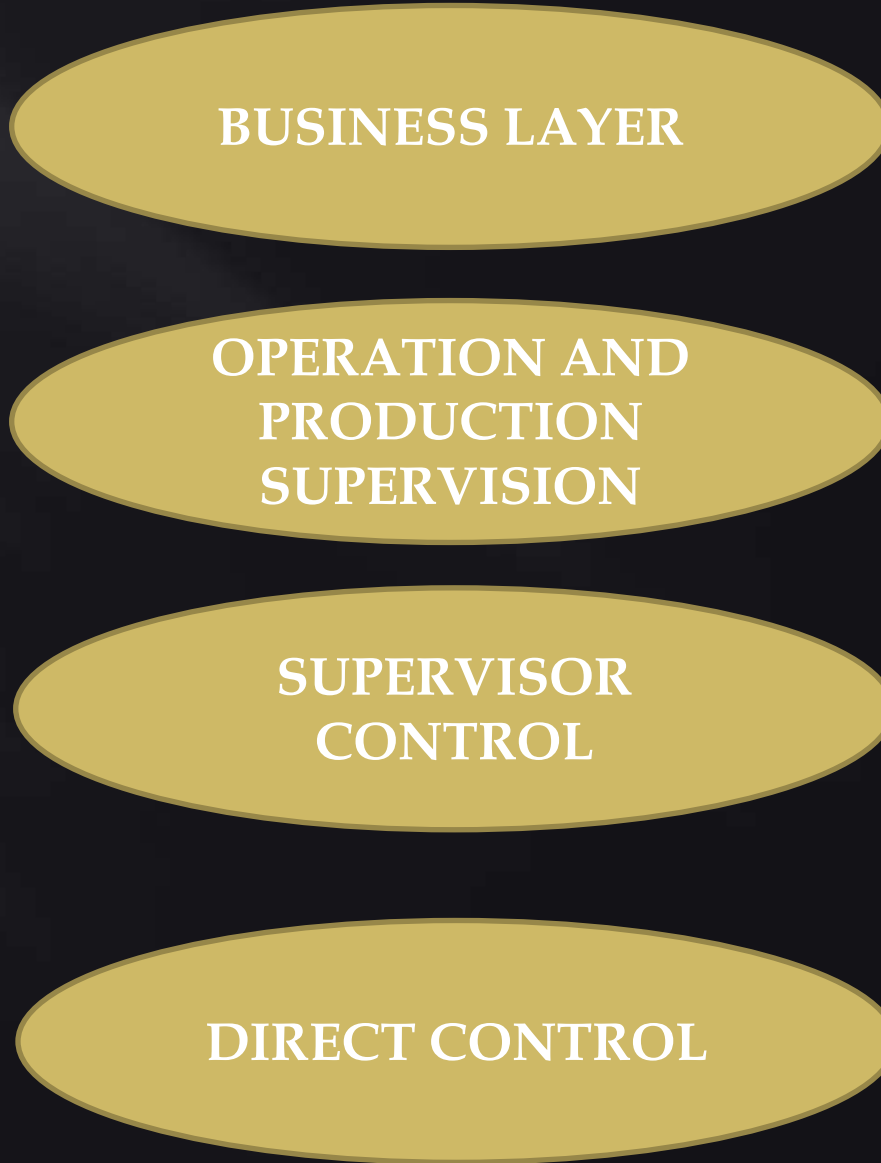
- ▣ Siemens ProductCERT
  - **Really** professional team
  - Quick responses
  - Personal contacts
  - Patches in 10-30 days
  
- ▣ **You guys rock!**

# ICS/SCADA Overview



# Industrial Control Systems

PLC/RTU   SCADA   MES   ERP



# Current trends

- **NO magic** on network
  - Standard network protocols/channel level
- **NO magic** on system level
  - Standard OS/DBMS/APPs
    - Windows/SQL for SCADA
    - Linux/QNX for PLC
- ICS guys don't care about IT/IS
- MES reality - connect SCADA to other networks/systems (ERP etc.)

# SCADA network puzzle





# ICS Transports

- Ethernet
- Cell (GSM, GPRS, ...)
- RS-232/485
- Wi-Fi
- ZigBee
- Lot's of other radio and wire
- **All can be sniffed thanks to community**

# Protocols: Welcome to the Zoo

- Modbus
- DNP3
- OPC
- S7
  
- **And more and more ...**
- EtherCAT
- FL-net
- Foundation Fieldbus

# Playing with...

- Sniffing
- Spoofing/Injection
- Fingerprinting/Data collection
- Fuzzing
- Security?! – OPC, DNP3

# Sniffing

- ▣ Wireshark supports most of it
- ▣ Third-party protocol dissectors for Wireshark
- ▣ Industry grade tools and their free functions
  - FTE NetDecoder
- ▣ No dissector/tool – No problem
  - Plaintext and easy to understand protocols

# Spoofing/Injection

- ▣ Widely available tools for Modbus packet crafting
- ▣ Other protocols only with general packet crafters (Scapy)
- ▣ More tools to come (from us ;))
- ▣ Most of protocols can be attacked by simple packet replay

# Fingerprinting/Data collection

- ▣ Well known ports
- ▣ Modbus
  - Product, Device, GW, Unit enumeration
- ▣ S7
  - Product, Device, Associated devices
- ▣ OPC
  - RPC/DCOM
- ▣ Modern fingerprinting add ons
  - snmp, http, management ports

# PLC Scan

- ▣ Open Source ICS devices scan/fingerprint tool
- ▣ Support modbus, S7, more to come
  - Software and hardware version
  - Device name and manufacturing
  - Other technical info
- ▣ Thank to Dmitry Efanov

# PLC Scan

## Siemens PLC

127.0.0.1:102 S7comm (src\_tsap=0x100, dst\_tsap=0x102)

Module : 6ES7 151-8AB01-0AB0 v.0.2  
Basic Hardware : 6ES7 151-8AB01-0AB0 v.0.2  
Basic Firmware : v.3.2.6  
Unknown (129) : Boot Loader A  
Name of the PLC : SIMATIC 300(xxxxxxxxxx)  
Name of the module : IM151-8 PN/DP CPU  
Plant identification :  
Copyright : Original Siemens Equipment  
Serial number of module : S C-BOUVxxxxxxxx  
Module type name : IM151-8 PN/DP CPU

## Modbus device

127.0.0.1:502 Modbus/TCP

Unit ID: 0

Response error: ILLEGAL FUNCTION

Device info error: ILLEGAL FUNCTION

Unit ID: 255

Response error: GATEWAY TARGET DEVICE FAILED TO RESPOND

Device: Lantronix I WiPo V3.2.25





Demo

PLC Scan the Internet

# Who is mister PLC?



# PLC

- ▣ Just a network device with it's own
  - OS
  - Network stack
  - Applications
  - ...vulnerabilities
- ▣ How to find vulnerabilities in PLC
  - Nothing special
  - Fuzzing
  - Code analysis (MWSL?)
  - Firmware reversing

# Vulnerabilities

- ▣ Hardcoded SSL CA certificate (Dmitry Sklarov)

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

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

[http://www.siemens.com/corporate-technology/pool/de/forschungsfelder/siemens\\_security\\_advisory\\_ssa-279823.pdf](http://www.siemens.com/corporate-technology/pool/de/forschungsfelder/siemens_security_advisory_ssa-279823.pdf)



Demo

Root via PUT

# Miss SCADA



# Components

- Network stack
  - Connects with PLCs, etc
- OS
- Database
- Applications
  - HMI
  - Web
  - Tools

# Built-in Security

- ▣ Depends on OS/DBMS security
  - GUI restrictions/Kiosk mode for HMI
  - OS network stack and API heavily used
    - ▣ File shares
    - ▣ RPC/DCOM
    - ▣ Database replication
- ▣ Password authentication, ACLs/RBAC
- ▣ Something else?



# OS Level

- Nothing special
  - Windows/Linux
  - No Patches
  - Weak/ Absence-of Passwords
  - Misconfiguration
  - Insecure defaults

# Database Level

- Insecurity configuration
- Users/password
- Configuration
- ICS-related data

# WinCC – Database Security

- Hardcoded accounts (fixed in SP3)
- 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
- Database for new project created based on txt template
  - Perfect place to hide\*

\*make a note

# WinCC accounts

- Managed by UM app
- Stored in dbo.PW\_USER

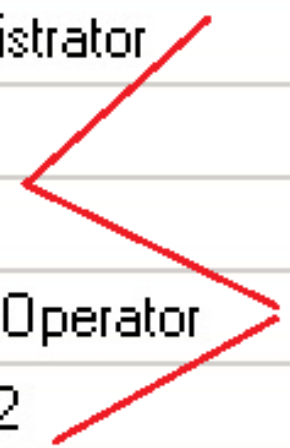
```
select ID, NAME, PASS, CAST(PASS as varbinary) from dbo.PW_USER
```

Results Messages

ID	NAME	PASS	(No column name)
10	Administrator	!.'>k&a0rq;cn7 8\$;:	0x142E273E6826613072713A636F372038243B3B202020202...
11	Avgur	!<.'1&>p_M0	0x143C2D2231263E705F4D1220202020202020202020202...
12	Admin	!.'>kot(ds!w)WGO	0x142E273E686F7428647311575D57474F202020202020202...
13	LogonOperator	!%-8_0Q !t*<	0x19252D385F1410510A0E742A3C2020202020202020202...
14	Avgur2	!<.'w]0o !Q\	0x143C2D22775D306F202912515C2020202020202020202...

# 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
```

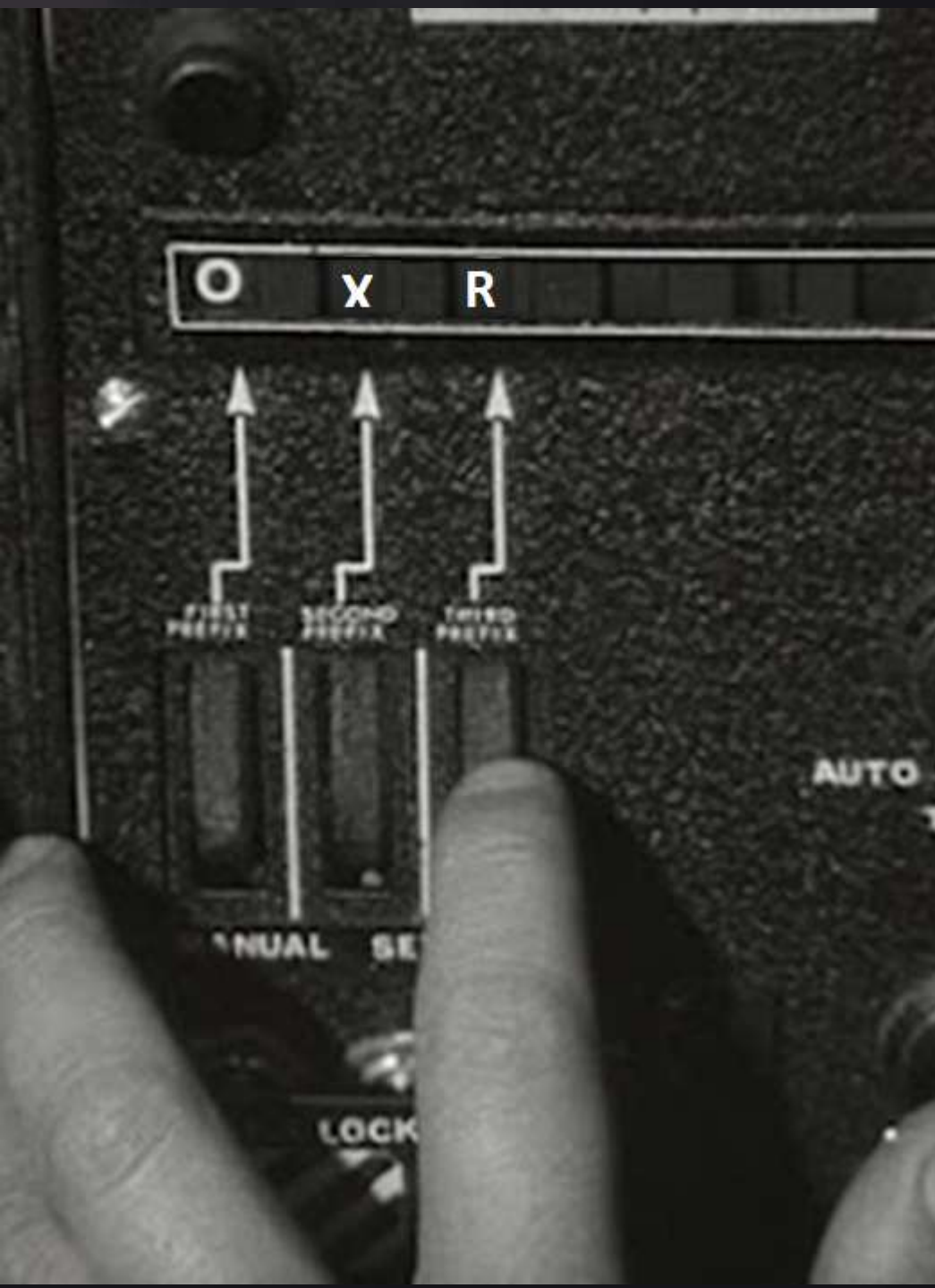
```
; DATA XREF: sub_4478C0+2C0↑r
sub_447CE0+11B↑r
"This is my encryptionkey"
```





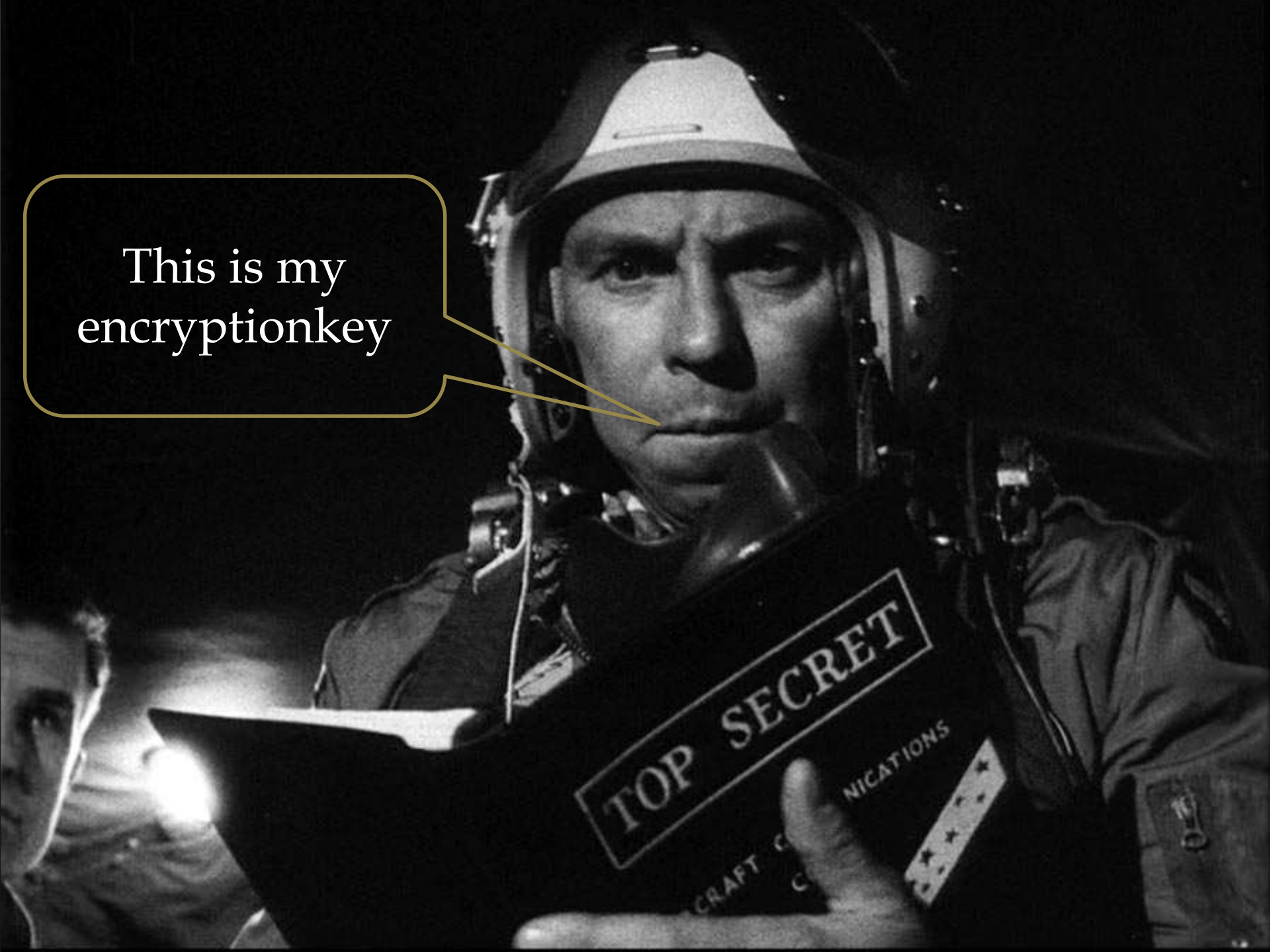


First one  
to guess  
the cipher  
gets...



...  
exclusive  
T-shirt or  
free beer!

This is my  
encryptionkey





How to decrypt?

We don't know yet...



...responsible disclosure

# Releases

- ▣ WinCC OS/database forensic white paper and script
- ▣ WinCC security hardening guide
- ▣ **Exclusive** cipher tool & msf module. We don't have yet...

Demo



SCADA forensic with MSFT

# Heavy Weapon





# WinCC Applications

- ▣ WebNavigator
  - Web-based HMI
  - IIS/ASP.NET
  - ActiveX client-side
- ▣ DiagAgent
  - Diagnostic and remote management application
  - Custom web-server
- ▣ ...

# 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) {
```

# DiagAgent

- ▣ Not started by default and shouldn't never be launched
- ▣ No authentication at all
- ▣ XSSes
- ▣ Path Traversal (arbitrary file reading)
- ▣ Buffer overflow

## 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].

# WebNavigator

- ▣ Web-based HMI
- ▣ **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?

\* <http://www.slideshare.net/phdays/root-via-xss-10716726>

# Client-side WinCC Fingerprint

[Русский | English]



 <b>Internet Explorer, 9.0.8112.16421</b> Medium risk >	<b>Recommendations</b>
 <b>Java Runtime, 1.7.0.5</b> >	<b>OK!</b>
 <b>Adobe Reader Plugin, 10.1.0</b> >	<b>OK!</b>
 <b>Adobe Flash Player, 11.3.300.257</b> >	<b>OK!</b>
 <b>Windows Media Player, 12.0.7601.17514</b> >	<b>OK!</b>
 <b>Siemens SIMATIC WinCC HMI ActiveX</b> Medium risk >	<b>Recommendations</b>

Please pass your opinion: ☆☆☆☆☆

You should never underestimate  
the predictability of ...

Is there any other bugs in WinCC?





# Such as...

- ▣ Lot of XSS and CSRF
  - CVE-2012-3031
  - CVE-2012-3028
- ▣ Arbitrary file reading
  - CVE-2012-3030
- ▣ SQL injection over SOAP
  - CVE-2012-3032
- ▣ Username and password
  - CVE-2012-3034

<http://scadastrangelove.blogspot.com/2012/09/new-vulnerabilities-in-siemens-simatic.html>



# Such as...

- ▣ Username bruteforce?
- ▣ Password disclosure?
- ▣ Path traversal?
- ▣ Arbitrary file reading?
- ▣ SQL injection?
- ▣ XSS?



We don't know yet



...responsible disclosure

Demo



PS

First time we ...

We're inspired

But... It's peace of cake



It's low hanging fruits







And this is scaring



**SCADA STRANGE LOVE OR:  
HOW I LEARNED TO START WORRYING  
AND LOVE NUCLEAR PLANTS**

***SCADASTRANGELOVE.ORG***