

Exploiting SCADA Systems





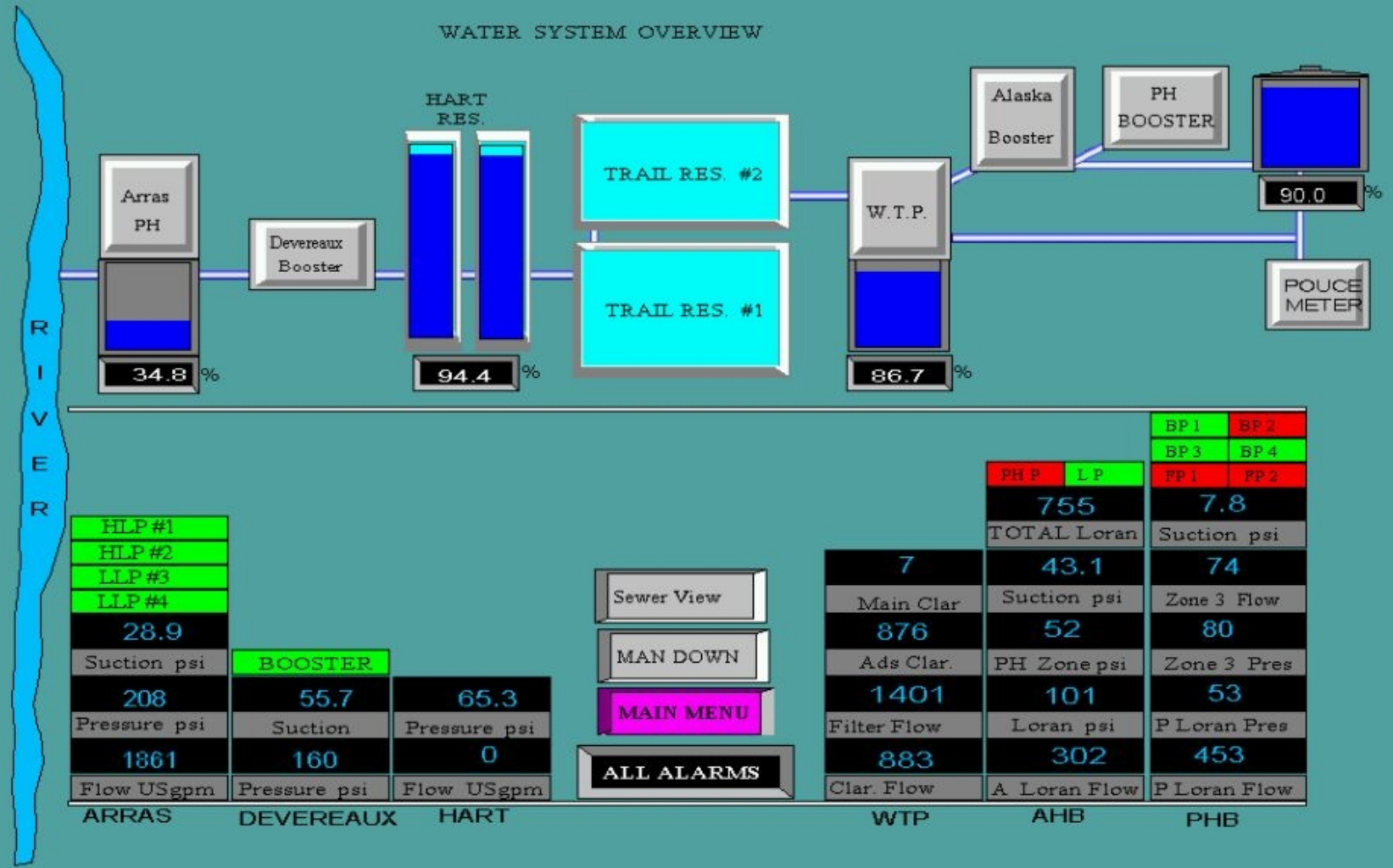
What is SCADA?



Supervisory Control and Data Acquisition



WATER SYSTEM OVERVIEW



HLP #1		
HLP #2		
LLP #3		
LLP #4		
28.9		
Suction psi	BOOSTER	
208	55.7	65.3
Pressure psi	Suction	Pressure psi
1861	160	0
Flow USgpm	Pressure psi	Flow USgpm
ARRAS	DEVEREAUX	HART

- Sewer View
- MAN DOWN
- MAIN MENU**
- ALL ALARMS

7	PH P	LP	BP 1	BP 2
Main Clar	755		BP 3	BP 4
876	TOTAL Loran		PP 1	PP 2
Ads Clar.	43.1		7.8	
1401	Suction psi		74	
Filter Flow	52		Zone 3 Flow	
883	PH Zone psi		80	
Clar. Flow	101		Zone 3 Pres	
	Loran psi		53	
	302		P Loran Pres	
	A Loran Flow		453	
	P Loran Flow			
WTP	AHB		PHB	



3G 9:42 AM

Tags

GENERAL

Main Run/Stop Switch ON
Main Process Start/Stop

WATER TANK

Tank Level (L) 388.712
Water Tank Current Level

Output Flow (L/s) 13.448
Current Output Flow from Tank

High Level Set Point (L) 902.499
Level at which pumps stop

Mid Level Set Point (L) 400.89
Level at which pump 1 stops

Low Level Set Point (L) 106.344
Level at which pumps start

VALVE 1

Limit Switch OPEN
Valve 1 Completely Open

Limit Switch OFF
Valve 1 Completely Closed



Who uses SCADA?



Factories





Nuclear Plants





Airports





Space Stations





You



X10 Commander

- Basement Lights
- Bedroom Lamp
- Garage Door
- Home Theater Lights
- Kitchen Lights

ON **OFF**



DIM Connected to 192.168.1.103:6003 **BRIGHT**





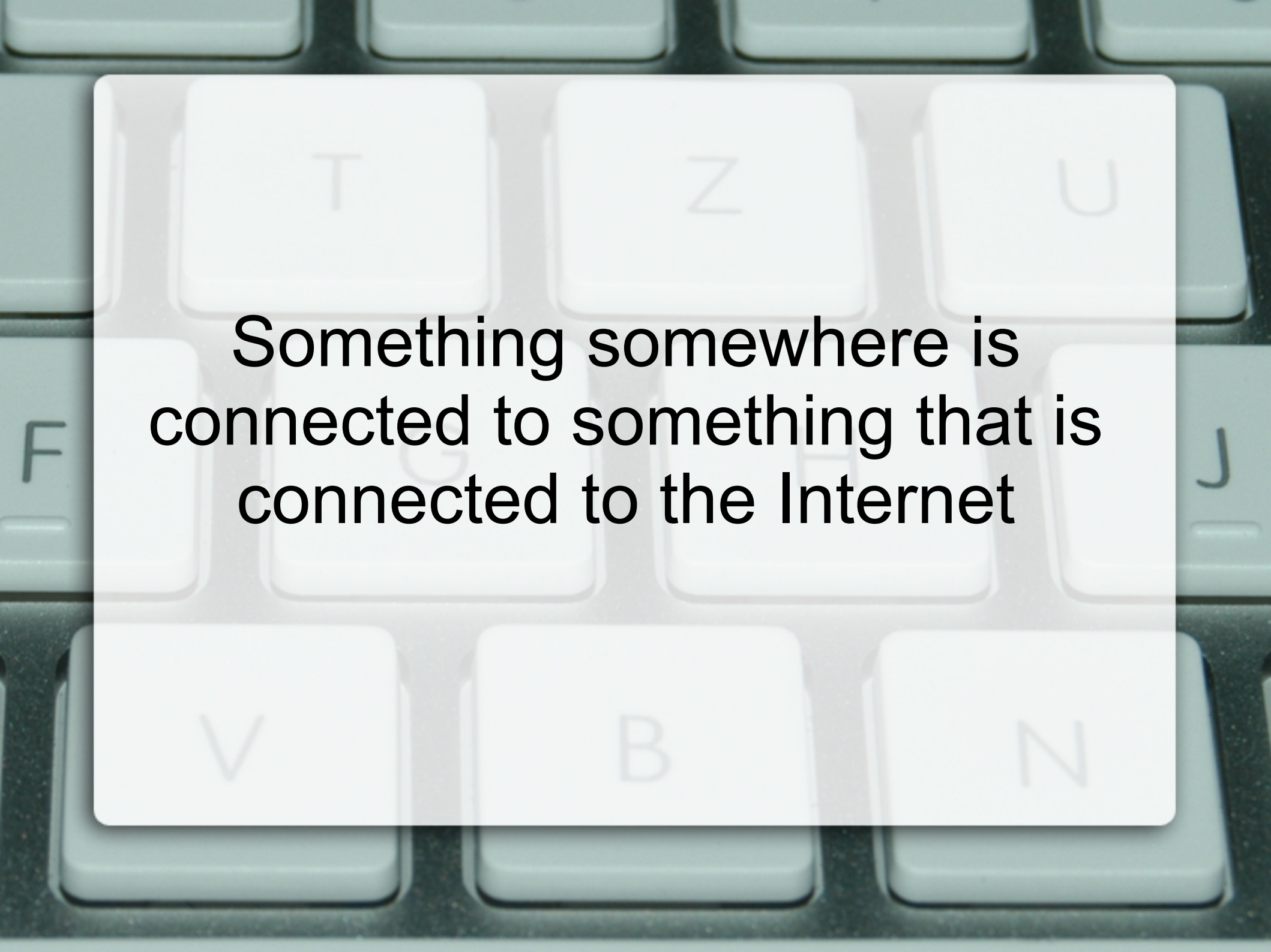
**Why are SCADA systems
vulnerable?**



No Anti-Virus Software




**Little authentication, sharing of
credentials**



**Something somewhere is
connected to something that is
connected to the Internet**

Security has been implemented
as an add-on instead of being
built around the product from the
ground up



Vendors take their time with updates, managers take their time updating



SCADA Components

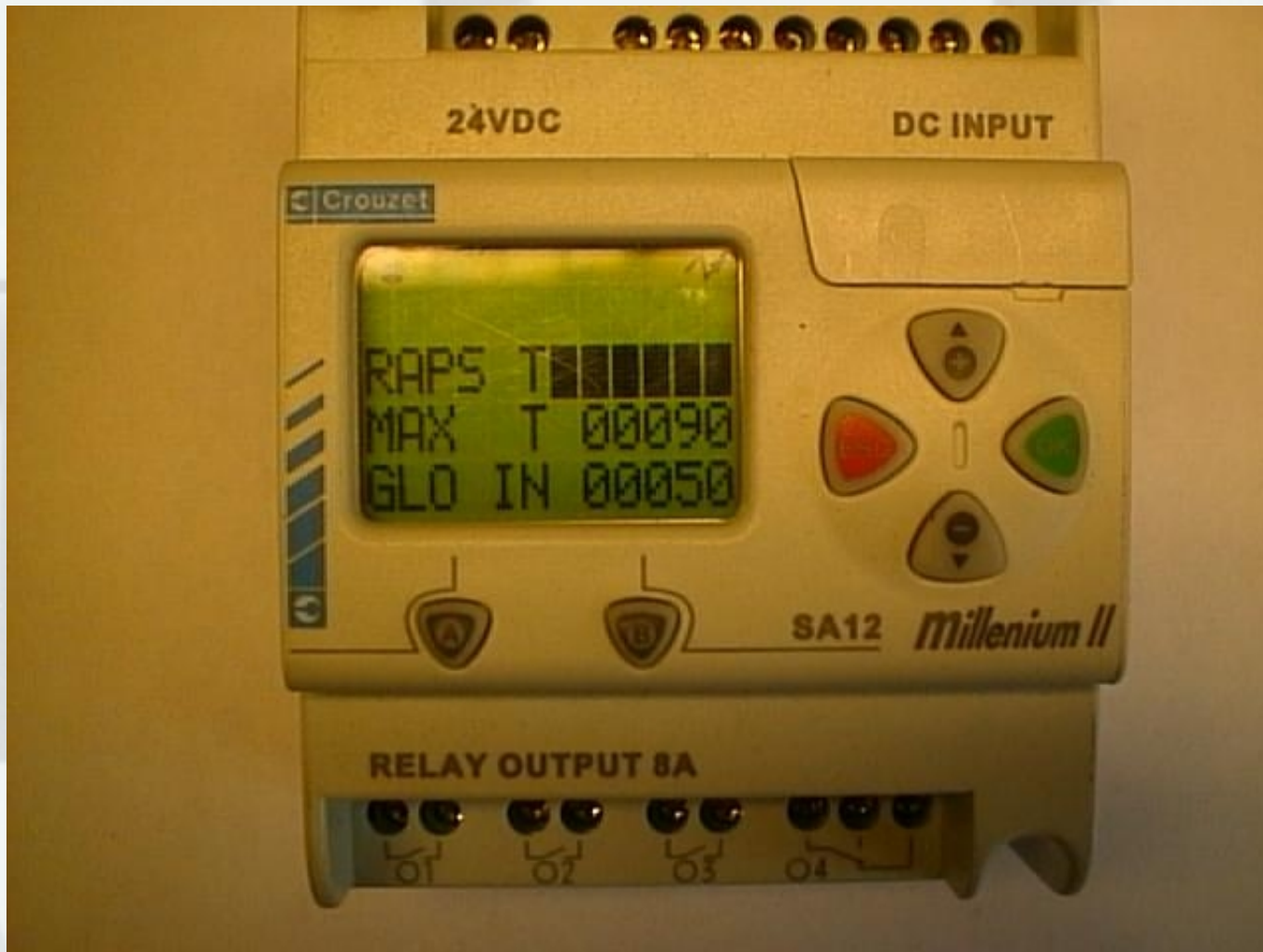
RTU

Remote Terminal Unit



PLC

Programmable Logic Controller



HMI

Human Machine Interface





Who abuses SCADA?



Employees





Hackers (up to no good)





Security Professionals

KEVIN JAMES



PAUL BLART
MALL★COP

SAFETY NEVER TAKES A HOLIDAY

JANUARY 16

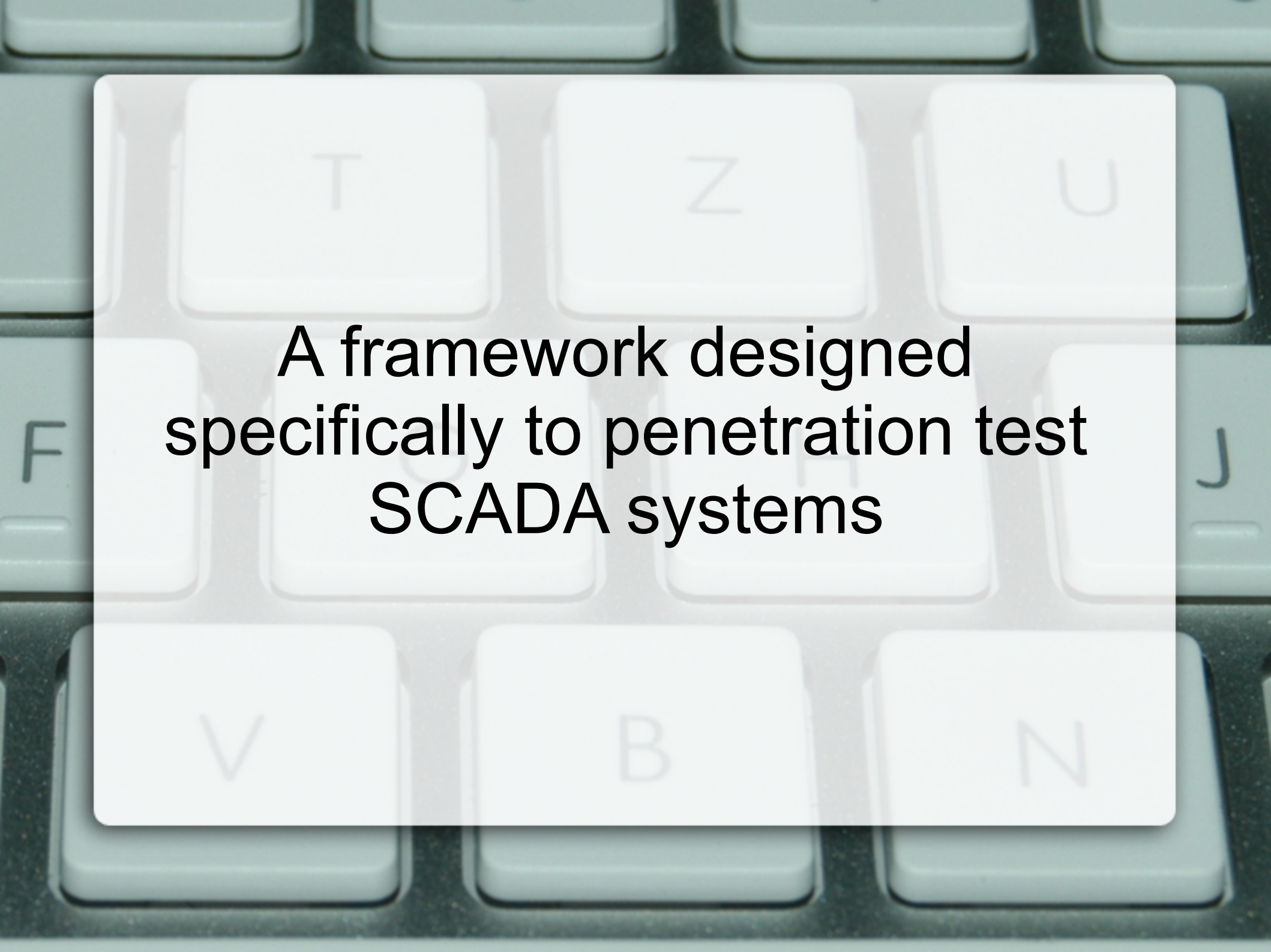


You?





Sploitware



**A framework designed
specifically to penetration test
SCADA systems**



**Can check SCADA systems for
0day vulnerabilities**



Exploitation is optional but readily available

Similar concept to CANVAS,
VulnDisco, and Core Impact yet
focused on SCADA software

DEMO!



Conclusion

**SCADA software is just as
vulnerable as your typical
download.com software**



Windows



Windows

Mac

Mobile

Webware

ad Save up to \$300/year on phone bills

Home > Windows Downloads > Antivirus, Firewall, & Spyware > Antivirus Software

Windows Software

Audio & Video Software

Antivirus, Firewall, & Spyware

Utilities & Drivers

Graphic Design Tools

Screensavers & Wallpaper

Business Software

Productivity Software

Browse Download for more popular software

People who downloaded SafeSpace Free Edition also downloaded:

- 1. Assassin**
Protect your PC from harmful threats.
- 2. AntiVirus Defender**
Protect your computer from viruses and malware.
- 3. Dynamic Security Agent**
Protect your Windows desktops and servers from malware and intrusions.

All most popular downloads

- 1. AVG Anti-Virus Free Edition**
Protect your computer from viruses and malicious programs.
- 2. LimeWire**
Share files online.
- 3. Ad-Aware 2008**
Protect your personal home computer from malware attacks.

Downloads from our sponsors

Sponsored Links

[Block Trojan Attacks](#)

Protect your network from email viruses & trojans with MailSecurity
www.gfi.com

[Your PC is infected ?](#)

Scan your PC for free. Download and try Noadware for free.
www.noadware.net



Thank you

