

PenTest

magazine

Aud & Stand

50+
PAGES

Vol.2 No.1 Monthly ISSN 2084-1116
Issue 01/2013(10) February

SCADA

THREATS, HACKERS & HOW TO PROTECT AGAINST THEM

BY ALAN GRAU FROM ICON LABS

STUXNET MADE US AWARE!

BY ROB HULSEBOS

HOW HACKERS GET CAUGHT: THE TRUE STORY

BY AB CONSULTANCY SOFTWARE SRL

PLUS

INTERVIEW WITH
DAN BRABEC
BUSINESS MANAGER,
SCADA PRODUCTS,
MOTOROLA
SOLUTIONS

AnDevCon

The Android Developer Conference

BOSTON • May 28-31, 2013

The Westin Boston Waterfront

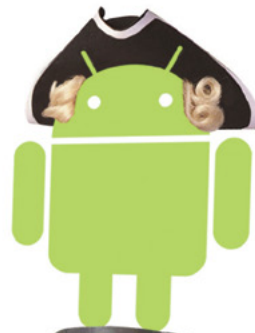
Get the best real-world Android developer training anywhere!

- Choose from more than 75 classes and tutorials
- Network with speakers and other Android developers
- Check out more than 40 exhibiting companies

Register Now
and SAVE!

“AnDevCon is one of the best networking and information hubs available to Android developers.”

—Nate Vogt, Android Developer, Willow Tree Apps



Register NOW at www.AnDevCon.com

A BZ Media Event

Follow us: twitter.com/AnDevCon

AnDevCon™ is a trademark of BZ Media LLC. Android™ is a trademark of Google Inc. Google's Android Robot is used under terms of the Creative Commons 3.0 Attribution License.

DIAMA¹³

digital marketing & advertising showcase

THE TRENDS & THE FUTURE

www.madverts.asia

Concurrently held with:



Running Alongside:



Organized by:



Endorsed by:



Segment Sponsor:



Supported by:



Media Partners:



Primary Highlight:



Government Technologies Showcase

An Insight into Asia Pacific Government Best Practices

www.govtechshow.com

Concurrently held with:



Running Alongside:



Organized by:



Endorsed by:



Supported by:



Media Partners:



20 - 21 March 2013

Putra World Trade Centre, Kuala Lumpur, Malaysia

For more information, call us at +603 2600 6000 or email us at marketing@jfpsgroup.com

MOBILE & WIRELESS TECHNOLOGY

www.mobilewirelesstech.com

Shaping the Future of Asia Pacific Connected Devices

Concurrently held with:



Running Alongside:



Organized by:



Endorsed by:



Supported by:



Media Partners:



Primary Highlight:



We're Back!

This 2ND EDITION is Deemed To Be Bigger!

ISWec 2013

Infosecurity World Exhibition & Conference

www.infosecurityworld.net

Concurrently held with:



Running Alongside:



Organized by:



Endorsed by:



Supported by:



Media Partners:



PenTest magazine

A
u
d
&
S
t
a
n
d

TEAM

Managing Editor: Bartosz Majkowski
bartosz.majkowski@software.com.pl

Associate Editors: Łukasz Gierałtowski, Patrycja Przybyłowicz

Betatesters / Proofreaders: Artem Shishkin, Donald Iverson, Ewa Duranc, Stefanus Natahusada, Tzvi Spitz, Vaman Kini, Jeff Weaver

Senior Consultant/Publisher: Paweł Marciniak

CEO: Ewa Dudzic
ewa.dudzic@software.com.pl


Art Director: Ireneusz Pogroszewski
ireneusz.pogroszewski@software.com.pl
DTP: Ireneusz Pogroszewski

Production Director: Andrzej Kuca
andrzej.kuca@software.com.pl

Marketing Director: Ewa Dudzic
ewa.dudzic@software.com.pl

Publisher: Software Media Sp. z o.o.
ul. Bokserska 1, 02-682 Warszawa
Phone: +48 22 427 36 56
www.pentestmag.com

Whilst every effort has been made to ensure the high quality of the magazine, the editors make no warranty, express or implied, concerning the results of content usage. All trade marks presented in the magazine were used only for informative purposes.

All rights to trade marks presented in the magazine are reserved by the companies which own them. To create graphs and diagrams we used [smartdraw.com](http://www.smartdraw.com) program by  SmartDraw

Mathematical formulas created by Design Science MathType™

DISCLAIMER!

The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

Dear Readers,

We present you our new PenTest Auditing&Standards. This issue is dedicated to Supervisory Control and Data Acquisition, but you will find in this issue two additional articles on a different topic that you might consider interesting. Also, we have a special guest from Motorola. Check our interview out to know him better!

We open the issue with an article by Larry Karisny who describes how new processes require new cybersecurity solutions. Larry briefly presents experts' opinions on the matter. Among those experts you will find: Joe Weiss, Patrick Miller, Vint Cert, Rajev Bhargava, Paul Sobel, and Curt Massey. Don't skip it. We recommend it as a first read!

Next, you should take a look at Rob Hulsebos' article – Pentesting SCADA, which should be important for everyone who is into Stuxnet. He states that: "SCADA has become a hot topic, not just for the vulnerabilities in industrial systems, but due to the connection with national infrastructure (electricity, water, gas, hospitals, airports), cyberterrorism and cyberwarfare. The consequences of a successful "SCADA hack" may thus be disastrous."

Moving further with your read you will discover more and more in SCADA Step by Step section. From Austin Scott's article you will have an opportunity to learn how to define industrial control systems with data diodes. He will explore the inner workings and practical control system applications of these unidirectional gateways. He will also provide a step by step guide to create your own using Open Source.

At the end of section you will find an article written by Alan Grau from Icon Labs: SCADA Security Device – Threats, Hackers, and How to Protect Against Them.

The last section dedicated to SCADA topic is an interview, where you will meet our special guest Dan Brabec, from Motorola Solutions. Check out why we have chosen him and what interesting he has to tell you.

Further, you will be provided with Albert Whale's article on homeland security, which we are sure you will find interesting although it doesn't refer to SCADA directly.

We close the issue with section titled: Extras. Here we placed two additional articles. The first one is a case study devoted to rootkits: How Hackers Get Caught: the True Story from AB Consultancy Software SRL. The second is dedicated to telecom operators and security concerning this topic.

We hope that you will find this issue worthwhile. If you enjoyed the articles from section Extras and you would like us to prepare the full issue about telecom or rootkits, please write contact us at en@pentestmag.com and let us know about it!

Enjoy your reading!

Thank you all for your great support and invaluable help.

Bartosz Majkowski
& PenTest Team

A BRIEF INTRODUCTION TO SCADA SYSTEM

SCADA, New Processes Require New Cyber Security Solutions 06

By Larry Karisny from ProjectSafety.org

With cyber war now verified and eminent, it is imperative to protect the heart of critical infrastructure security weakness, SCADA. We must act quickly and accurately and today's cybersecurity solutions may not be up to the task. Following is a review of what security architectures will work and which legacy architectures may not work in today's new cyber cold war. Check what experts think about this!

Pentesting SCADA 10

By Rob Hulsebos

Since 2010, Stuxnet made us aware of the lack of cyberquality in industrial systems. Until that year, industrial systems were largely ignored by hackers and the cybersecurity industry. Since then, "SCADA" has become a hot topic, not just for the vulnerabilities in industrial systems, but due to the connection with national infrastructure (electricity, water, gas, hospitals, airports), cyberterrorism and cyberwarfare. The consequences of a successful "SCADA hack" may thus be disastrous. The Netherlands learned this in the beginning of 2012, when a pentester discovered that remote control of sluices was possible.

SCADA STEP BY STEP GUIDE

Defending Industrial Control Systems with Data Diodes 16

By Austin Scott from Synergist SCADA Inc

Originally designed by government organizations to protect top secret information, data diodes are most commonly used in applications requiring the highest level of security such as state secret protection, banking or battlefield up-links. In recent years we could observe an increasing demand for data diodes in the world of industrial control and automation to protect critical infrastructure due to the simple and virtually impenetrable nature of these devices. In this article the author explores the inner workings and practical control system applications of these unidirectional gateways and provide a step by step guide to creating your own using open source software.

SCADA Device Security – Threats, Hackers and How to Protect Against Them 24

By Alan Grau from Icon Labs

SCADA protocols themselves are often inherently insecure. They may lack basic security measures. Instead they often rely on "security by obscurity" or on isolation from public networks for security. Without security measures such as authentication and encryption, the underlying protocols provide an

easy avenue for hackers wishing to attack SCADA devices. Firewalls provide a simple and effective layer of security and have long been used to protect home and enterprise networks. A small, SCADA aware firewall can be used to protect devices in SCADA devices from a wide range of cyber-attacks.

INTERVIEW

The Interview with Dan Brabec, Business Manager of SCADA Products at Motorola Solutions 30

By PenTest Team

Motorola has been a provider of SCADA solutions for over 40 years. They have been a pioneer in the intelligent use of radio for control systems. Read about how Motorola started, developed and what are their long term future plans. Get some tips on security, when running SCADA system at your company.

LET'S TALK ABOUT SECURITY

Homeland Security – Reducing the Thread from Attacks 34

By Albert Whale

This article is written to describe the changes being made in the Homeland Security activities for new software in development, and how they are improving our overall security. The reader may also find which activities can fit into their Software Development Lifecycle (SDLC) programs to further benefit other organizations as well. This is not an offensive approach to Cyber Security, but an improved defensive approach.

EXTRAS

How Hackers Get Caught the True Story 40

By AB Consultancy Software SRL

Most high-profile intrusions of the past decade haven't been found due to intrusion detection sensors or complicated forensic tools. Instead, it was the malfunctioning code in the rootkits that made them crash the system with weird error messages. Find out why the author states that current Unix anti-rootkit tools provide little to no accuracy in detection of rootkits, the impossibility to clean the system from a rootkit infection or the ability to analyze the malware.

Security Concern in "FemtoCell-Our own Base Station" 44

By Nitin Goplani

"Coverage" is a key term for all telecom operators. Providing coverage is always a challenge for them. Day by day mobile users are increasing and because of this growth mobile operators are very constraint for bandwidth. That's why we are facing coverage problem and sometimes unable to connect to mobile users in an emergency. The concept behind this problem is known as cell splitting.

SCADA

New Processes Require New Cyber Security Solutions

When working on upgrading our global power grid (Smart Grid), alarming security vulnerabilities were found in the supervisory control and data acquisition SCADA systems. These security vulnerabilities were so great that they initiated a US Presidential Executive orders to improve critical infrastructure cybersecurity. There is no question if there are security vulnerabilities.

There are and the heart of these vulnerabilities lies in SCADA operations. The true question is can current cybersecurity methodologies offer the impenetrable security required in protecting global critical infrastructure?

When discussing SCADA security vulnerabilities it is important know the the difference between supervisory control and data acquisition SCADA and industrial control system (ICS). Industrial control systems are computer controlled systems that monitor and control processes that are with in proximity of the the physical world (example: power grid substation). ICS cyber security expert Joe Weiss explained:

"Their primary function is to provide safe, reliable operation with computer operators and system integrators trained for reliable operation not security. From a cyber security perspective, the most important considerations are availability of the process and authentication of the devices; confidentiality is generally not important for the data "in motion." The concern is that inappropriate use of IT technologies,



policies, and/or testing such as penetration testing could, and has, impacted the performance of ICSs."

The heart of cyber vulnerability in our critical infrastructure today is SCADA. SCADA systems are an extension of both human and machine processes that interconnect many ICS systems to large scale processes that can include multiple sites and facility based process over large distances. The very definition of SCADA accentuates the security vulnerabilities being realized today. To effectively secure SCADA we must secure the extension of both the human business processes and IT system processes. In an earlier interview I had with Patrick Miller, CEO of Energy-Sec he explained:

"It isn't far from what I've heard from them over the past few years as we've ramped up the grid modernization efforts. Overall, the grid itself is highly resilient, but we are implementing new technologies and new connections without fully understanding the emergent issues that arise with this degree of innovation and complexity."



This interconnecting of control and data systems now need a network and if we want security it is not the Internet. Vint Cerf the father of the Internet stated:

“One of things incumbent on all of us is to introduce strong authentication into the fabric of the smart grid. We did not do that with the Internet.”



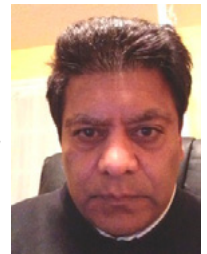
The Internet was built to be used as an large open shared medium and does not have the need characteristics required for needed security mandatory in critical infrastructure applications. These networks must be able to offer the ability to interconnect local and regional industrial control systems over private IP backbones. French network operator Sigfox considered this so important they are setting up of a separate, dedicated network specifically for machine-to-machine (M2M) communication for greater security and robustness of networks. Even these private networks would be plagued with current encryption key theft and mismanagement that is so great that entirety new methods of network security protection are beginning deployed. A dedicated network alone will not solve the security issues with SCADA.

The desire to digitize and interconnect critical infrastructure intelligence has great value. From greatly improving transportation traffic flow to saving trillions of dollars in energy consumption, the potential benefits are real and should not be ignored. There are those that would like to delay the needed upgrade to our power grid (smart grid) due to concerns with digital security. We cannot stop digital intelligence. In fact, its is not only a required for critical infrastructure efficiency it is required for critical infrastructure security. Digital intelligence is actually a part of security. For example, when first reviewing power grid vulnerability the US Department of Energy found that a single power grid operator could enter unmonitored facilities and manually take down entire parts of the grid by just pulling a switch. To correct this potential undetected take down of the grid, authentication access locks and video cameras were put in the many power grid facilities. This combination of human and digital actions will always be a part of our critical infrastructure.

The trick is how can we develop security technologies that can effectively view, detect, audit and secure SCADA human and machine business processes.

I always have issue with current Intrusion Prevention Detection Systems (IDS) and Intrusion Prevention Systems (IPS) security technologies because they are too focused securing networks and data. Don't get me wrong we need to protect the network and data theft. Cyber theft is becoming so prevalent that it was reported in 2011 to be a \$388 billion cybercrime business now as large as the international illegal drug trade. The problem seen in today's security is that we are using security technologies that were meant for casual personal PC use and now we are reaching data loads that are so great we can't even find proper analytic methodologies to measure them. My first suggestion would be is to start looking for what we need to secure and when do we actual detect it. Rajeev Bhargava is an acknowledged pioneer in the networking and software industry, and CEO of Toronto-based Decision Zone Inc. that offer a new way of addressing security. In a previous interview I asked him what is different about his approach. Mr. Bhargava stated:

“The act of observing or watching is always in the present. In the observing process, the activities are being watched with respect to the known logical business process. If the anomaly is known in the present, then it can be acted upon immediately and its impacts mitigated. The current IDS systems are predicting anomalies based on past analysis of data, and therefore cannot act on anomalies in the present. In other words, the current IDS systems require the full data record captured prior to analyzing the data element relationships within the data record for anomalies.”



If we can see ahead of the data the only other thing we need to do cover and encrypt the particular critical application we are sending. We must protect the networks and most importantly today the network application that we are sending. The biggest problem with today's IPS security

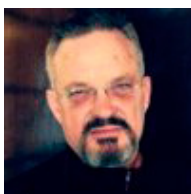
is that encryption keys have been stolen and mis-managed for years and can be seen on the network. From US Department of Defense contractors to those who job it was to secure encryption keys (RSA), no one is impervious to this serious problem. Aware of these encryption issues, Paul "Prem" Sobel a Cal Tech master of science in electrical engineering who has dedicated a 40-year career to protecting mission-critical systems. He earlier stated:

"In today's power-grid environment, we are connecting things that were never connected before, and they were never meant to be connected to the Internet. We are also working with old security architectures that can't scale to today's needs. These archaic systems do not address the complexity of SCADA control systems, and many were not built for network conductivity. The old ways won't work. Critical infrastructure security needs a fresh look. Mr. Sobel went on by explaining about a unique patented "encryption has never been broken. Encryption keys that disappear after they are used can't be compromised. It doesn't have to be complicated. It is a matter of using common sense."



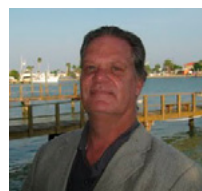
Curt Massey, CEO of STT (STTealth Shield) spent an entire 35-year career protecting United States national security. His military service, civilian law enforcement, corporate security and military contracting experiences have imbued him with the unpleasant knowledge of our core vulnerabilities. When asking him the question, Have you ever been breached, in any way, by any of the penetration testers or outright hackers who have gone up against your technology? He simply answered:

"No. You can't attack what you can't see... or touch. STT's network cloaking technology makes encryption invisible on the network." A simple but effective tool in IPS technology.



In summary, it seems clear that current legacy IPS and IDS security solutions are failing and will continue to fail if we do not give a fresh look as to how we are to secure SCADA control systems. These new and demanding security requirements seen in SCADA have presented critical infrastructure human and machine processes a whole new set of demanding security requirements. The needed solutions offer both challenges and opportunity in a new multi-billion dollar cyber security. It will be interesting to see in the near future just who meet and how will these challenges will be accomplished.

LARRY KARISNY



Larry Karisny is the director of Project Safety.org, a cyber security principle, advisor, consultant, writer and industry speaker focusing on security solutions for the smart grid and critical infrastructure. His 20 years of experience has includes network communication and integration work with companies such as Qwest Communications, WorldCom, Sprint and Microtel Corporation. He is currently Chief Business Development Officer for TLC Secure, a software security solutions provider serving the smart grid and critical infrastructure with security, privacy and identity management to multiple network applications. As Director of ProjectSafety, he has pioneered high-end wireless IPS and IDS security approaches insuring the safety of wireless smart grid, public safety, municipal wireless and various campus and enterprise applications. Larry Karisny has been a leading advocate for secure wireless smart grids, wireless end-to-end security, secure COTS interoperability standards and secured public/private network sharing, as well as a vision of the "smart city" of the future which will use technology to maximize efficient use of resources and enhance transportation, the environment and public safety.

Protected Only by Antivirus?

Complete your PC's security by running Malwarebytes Anti-Malware alongside your Anti-Virus to become fully protected from the latest threats.

Protect Your Business Now!

Visit [Malwarebytes.org](https://www.malwarebytes.org)



For more information,
Contact us at Corporate-Sales@Malwarebytes.org



Pentesting SCADA

Since Stuxnet there has been a lot of interest in the cybersecurity of industrial systems, usually called “SCADA”. Industrial IT is quite different in character from the office IT world. Any pentester operating in industrial environments should be aware of these differences, which may help in finding many easy security leaks.

Since 2010, Stuxnet made us aware of the lack of cyberquality in industrial systems. Until that year, industrial systems were largely ignored by hackers *and* the cybersecurity industry. Since then, “SCADA” has become a hot topic, not just for the vulnerabilities in industrial systems, but due to the connection with national infrastructure (electricity, water, gas, hospitals, airports), cyberterrorism and cyberwarfare. The consequences of a successful “SCADA hack” may thus be disastrous. The Netherlands learned this in the beginning of 2012, when a pentester discovered that remote control of sluices was possible. For a country where millions of people live up to 6 meters below sea level this is a frightening thought.

SCADA is the general word used in the cybersecurity world for anything resembling an industrial system. Technically this is not quite correct, since SCADA is often just a very small part of an industrial installation – the SCADA part is the operator’s user-interface and command panel, controlling from 1 up to dozens of PLC’s, I/O equipment, sensors, motors, frequency converters, robots etc. all controlled via an industrial Ethernet network or one of the many fieldbus protocols, and connected to the company LAN via a firewall or just a plain Ethernet connection. Add to this database systems, tracking & tracing storage, RFID, remote diagnostics capabili-

ties, wireless control, energy management, cooling, logistical systems, pneumatics and hydraulics and you get the idea what can be all meant by “SCADA”.

Why is a good definition of “SCADA” important? When a security researcher mentions to an industrial systems owner that his SCADA is cyber-unsafe, the message is completely misunderstood. The security researcher means: the complete factory is vulnerable, while the system owner understands: only the operator’s user interface (usually a PC) is vulnerable. The cybersecurity market and industrial IT are not on common ground (yet).

Industrial Attacks since Stuxnet

Since Stuxnet, many have tried to break into industrial equipment. Surprisingly easy, it has become very popular. One of the first researchers publishing results following the Stuxnet analysis was Luigi Auriemma (Italy). According to his own statement he just downloaded the demo-packages for 7 SCADA-packages from the vendor’s websites, worked on average 2 days on each one of them, and found 34 leaks – despite having no experience in SCADA at all. Interesting is his analysis of the rootcause of each leak, this helps us understand *why* such leaks exist. I have put all the results together in Figure1. It shows (for four vendors) what the rootcauses for all security leaks were. For ex-

ample, vendor B was badly plagued by input validation issues, and vendor D by buffer overflows.

When looking at the results in Table 1, I wonder why SCADA system D has so many buffer overflow issues, and B so many input validation problems. I suspect that these bugs were all coded by the same programmers, repeating the same implementation mistake again and again. This leaves the world with more than one million industrial applications being vulnerable to coding issues which we are taught not to make in a Programming 101 course. Unfortunately, popular programming languages used in industrial automation and embedded software, C and C++, are very susceptible to buffer overflows. Following Auriemma, many others have focussed on finding security leaks in industrial equipment, such as Digital Bond (see Figure 1). and others. The results are even more appalling, as can be read in a report by Positive Technologies (Russia), summarizing all industrial security incidents since 2005. It reports that in 2012 there were as security leaks as in the years 2005 thru 2011 *combined*. The fact that they can be so easily found is worrying, but makes pentesting particularly easy.

Why are Industrial Systems so Vulnerable?

The industrial IT world is quite different in attitude from the office IT world. To name a few differences:

- There are no major vendors as dominant as Microsoft is in office-IT. Instead, there are many smaller ones.
- Industrial IT goes at a much slower pace than office IT. Where the latter is now busy deploying Windows 8, in some industrial locations Windows XP is just arriving and occasionally even MSDOS is still run. Systems may be required to run 15-20 years, and get updated/modernized only after that period (or earlier, when they break down).

- Embedded software is used in lots of equipment. Every vendor uses his own style of writing software, own compilers, using all sorts of embedded OS's, network protocols, use of open-source products, different development and patch procedures, etc. Secure coding practices are scarce.
- Production is dominant. The main concern for the production staff is: production must continue. A single malfunctioning office-PC does not shut down a whole company, but a single failing PLC can stop a complete production line.
- It it works, don't touch it. Changes to the industrial IT systems are only applied when really necessary.

	AB QUALITY	Schneider Electric	GE	SEL	Koyo
Firmware	!	✗	!	!	!
Ladder Logic	!	!	✗	!	✗
Backdoors	!	✗	✗	✓	✓
Fuzzing	✗	✗	✗	!	!
Web	!	✗	N/A	N/A	✗
Basic Config	!	!	✗	!	!
Exhaustion	✓	✓	✗	✓	✓
Undoc Features	!	✗	✗	!	!

Figure 1. Security issues found in 5 SCADA systems.
Source: DigitalBond

Table 1. Results of the rootcause analysis by Auriemma for 28 security leaks found in four SCADA packages from vendors A, B, C and D

Bug #	A	B	C	D
1	Buffer overflow	Memory mgmt.	Input validation	Buffer overflow
2	Input validation	Input validation	Input validation	Buffer overflow
3	Memory Corruption	Integer overflow	Input validation	Buffer overflow
4	Buffer overflow	Input validation	Input validation	Buffer overflow
5	File I/O check	Input validation	Input validation	Buffer overflow
6	NULL pointer	Input validation	Printf bug	Integer overflow
7		Input validation	Buffer overflow	Buffer overflow
8		Input validation	Input validation	

- Industrial IT systems are often maintained by production personnel, who do not have an IT background and are not current with IT technology and cybersecurity.

Knowing these special characteristics of industrial IT gives us an insight into the specific vulnerabilities that a pentester could address. We will discuss these vulnerabilities in more detail.

Knowledge

Many industrial systems are maintained by production staff, who generally have no IT background and are not current with modern technology and their cybersecurity aspects. Their overriding concern is to keep production going, and there is no management attention, no time, no money and no knowledge available to keep a system cybersafe.

However, cybersecurity awareness is not completely lacking. When a completely new production system is installed it is now normal to require that it is properly protected. But without active maintenance the cybersecurity quality quickly deteriorates. A pentester should make an inventory of all equipment, and check whether they have been last upgraded. Very likely there is no up-to-date overview present, and it will take quite some time to make this overview. Do not rely on the original drawings, as changes are often applied without updating documentation. Physically check the systems involved for presence of network connections, new equipment, wireless links, etc.

The lack of security awareness of the staff is also a good entrypoint for a pentest, such as distributing USB-sticks on parking lots. Very likely all industrial PC's in a production line will have active "admin" accounts with no password, or one that is written down. Staff is also used to vendors visiting the production line and plugging their own service-laptops in the local factory network. I once connected a laptop with a DHCP server still running (accidentally). It took three hours before they found out why nobody could do useful work anymore.

Patching Frequency

Everything that has software in it is updated / patched regularly. The first thing one does with new equipment is check whether it has the latest firmware and patches installed. In industrial IT, patches released later do not get automatically installed. Very often, customers do not know of the existence of certain patches, since the vendor does not tell them. Also,

customers often do not actively search for patches, due to lack of time and production pressure.

Even when a patch is found by everyone to be essential, it remains to be seen when it is installed. This often requires downloading software (perhaps by a 9600 bit/s RS232 connection), and a reboot. During all this time the device is not available for production purposes. Installation of patches is therefore only done during production stops, sometimes in the weekend, sometimes in the week following Christmas, and sometimes only during the 2 or 5-yearly overhaul. I once worked on a customer's site where systems could only be updated during 1 hour every Sunday morning, when the operators went to church and production was halted.

Update Pace

Industrial PC's still running Windows NT or 2000 are even more at risk. These versions are phased out in the office IT, but are still quite common in industrial environments. Since Microsoft has stopped updating NT, 2000 and the oldest XP versions, they are vulnerable to almost all security issues found in the last decade. If I were to pentest such systems, I'd dust off all old exploits for Windows, Internet Explorer, SQLServer, Acrobat, Flash, Java, etc. and try them. Success guaranteed!

The question remains, why are these old systems not replaced? The reason is usually: it still works fine, and any upgrade requires a substantial investment in hardware and software, and carries the risk that production will suffer. So unless it is really, really, *really* necessary.. nothing changes. This used to be no problem in the past, but the fast changing cybersecurity world requires a different approach. For the time being, a good starting point for a pentest would be to target these old PC's.

Vendor Backdoors

A special class of security vulnerabilities is the presence of vendor-enabled backdoors in software. These are not meant for hacking, but usually for remote diagnostic support. For example, telnet, RDP or VNC.

The reason for this is simple: while a normal office will continue to function if one employee-PC is out of order, a production line controlled by 20 PLC's requires that *all* of these are operational 24/7 since a production line cannot operate if one manufacturing step is not executed. Diagnostic capabilities are a must; any malfunction must be resolved as soon as possible, to have production

continue. Many vendors have built-in remote diagnostic capabilities in their products to remotely assist the customers in finding the root causes or problems. Access to the equipment is (nowadays) usually via internet, but in the more remote parts of the world modem lines are still being used.

Another aspect of remote diagnostic capabilities is that they are often weakly protected. Many vendors just add a basic protection mechanism, for example a standard password that is identical worldwide, or a password generated based on some unique identifier (usually an Ethernet MAC-address or a serial number). It thus comes as no surprise that in 2011 and 2012 several vendors (for example, Siemens and RuggedCom) were found to sell equipment being vulnerable this way.

A pentest on an industrial system should always take the remote diagnostics functions into account. Even when the user (or the vendor!) states that there are no remote backdoors, very likely they do exist (especially if there are Ethernet ports). Many vendors do not disclose the existence of remote diagnostics capabilities to customers, and even when they do, customers may still be totally unaware of remote access capabilities. And even when they are: in case of a production stop, the overriding concern is to have it start again. Remote access functions that are ordinarily disabled may be quickly enabled to allow a vendor to assist remotely, but should be disabled again when no longer needed. Of course, this is easily forgotten in the aftermath of getting production rolling again.

Since remote diagnostic functionality can only be effective when total remote control of a device is possible (to solve any possible problem), very often root/superuser/admin-privileges are available. In 2011, PLC's of various vendors were found to be internally based on Linux. With superuser access, total control of the inner working of the PLC is possible.

Vulnerability of Industrial Networks

In the industrial environment, there are many different protocols in use. I once tried to keep a list of all that I encountered, but stopped after counting more than 500. In the past every vendor launched his own protocol, only suitable for the own products. Starting in the 80's, attempts were made to standardize, and this gave us protocols like Profibus, CAN, Modbus, etc. and dozens of others as everybody again tried to set his own standard.

For pentesting purposes, it is both an advantage and a disadvantage that there are so many proto-

cols in daily use. With so many protocols in daily use, it is assured that a lot of them are vulnerable to the standard attack vectors like buffer overruns, range checks, denial of service, etc. But for an attack to be successful, one needs to find the right protocol and an exploit for it. The large number of protocols may be a blessing in disguise for industrial cybersafety. This explains why there is probably no exploit for an industrial protocol (at least, that I know of). For hackers, it is much easier to focus on Ethernet and the TCP/IP suite of protocols.

Most industrial networks have never been designed to take cybersecurity into account. Nodes on the network implicitly trust each other, and thus the commands / data they send. This is how Stuxnet operated: once inside the Siemens PLC it could use the Profibus/DP protocol to send new setpoints for the motors controller by frequency converters. Simply increasing the RPM of the motors destructed the uranium enrichment plant. Although there is a limited protection mechanism in Profibus/DP that there can be only one 'master' on the network, this didn't help in Stuxnet: the Siemens PLC was *the* master.

Is it difficult to think of a mechanism that could have helped to protect the frequency converters against the strange commands they received from their PLC via Profibus? No. The devices do not know in which environment they operate, and which configuration parameter settings or commands are damaging to the system they are part of – compare it to the switching of the headlights of your car, while driving at high speed during the night. Of course, the frequency converters in Iran could have been protected with a range check on the RPM setting. This won't protect the factory – Stuxnet would then be written to wildly vary the RPM-settings within the allowed range. Protection against this is possible of course, but adds a layer of complexity: can we expect that a simple device in an industrial application "knows" its entire environment? We can't, and thus it must implicitly trust the commands and data it receives from its master.

An example of the limited security awareness in industrial networks is the (now obsolete) Profibus/FMS protocol. It had the option to assign a password to objects it could remotely access. This sounds good, but the "password" is only one byte in size. Any attempt to access an object could of course easily try them all. It is not surprising that that this option in the protocol was never implemented by anyone; it remained a paper tiger.

Fuzzing

The dedicated hardware needed to connect to an industrial network is another factor that makes pentesting industrial networks more difficult (but not impossible). Actually it is surprising that there is so little activity in this field, as it is not difficult to make fuzzers for industrial network protocols. But would this be useful? In order to check whether a system is vulnerable, one needs to be physically present and connect your own system to the network to be tested. Nevertheless, a good protocol fuzzer would certainly be useful – for vendors to check both the robustness, *and* the cyberquality of their network products.

Fuzzing gets a second chance now that more and more industrial Ethernet protocols are being used. In order to connect to such networks, a standard Ethernet controller usually suffices. These are readily available. The only industrial protocol fuzzer that I know about is the one made by German students for ProfiNet, which is Ethernet-based.

Protection Mechanisms

It is probably clear that for the time being we can't count on industrial IT equipment having such high quality software that it is not vulnerable. Even in other IT worlds this is not possible, and new operating systems launched in the last decade (such as Android) show that we haven't learned much yet. But there is progress: the "Qubes" OS and Kaspersky's announcement of its own secure OS. But it will take time for these to be fully developed and deployed, if ever.

A big improvement would be to have the capability for "hot upgrading", that is: install new software on equipment without requiring a reboot, a restart or a functional stop. As this necessitates a production stop, industrial users wait too long with upgrading and this keeps their systems vulnerable.

Until then, protection must come from the outside. Two products targeted at protecting industrial systems look promising. The first product is the "Silent-Security" IDS by Security Matters (www.security-matters.eu). The IDS monitors the network traffic, and learns what is 'normal'. This learning phase can take from several hours to several days, depending on the regularity of the network traffic. It is here where industrial systems have an advantage, because most industrial software executes the same cycle continuously, and is thus very predictable.

The second product I want to mention is the Tofino firewall (www.tofinosecurity.com), which is

based on iptables, but has been extended with a management layer to greatly facilitate its use in industrial environments by non-security experts. The Tofino is becoming a de-facto standard industrial firewall, as many large industrial vendors sell it under their own name. The Tofino also has the capability to do DPI (Deep Packet Inspection) on the Modbus/TCP protocol messages. For example, it can only allow read-only Modbus/TCP traffic to certain parts of a device's registers, or only allow specific values to be written to registers.

Pentesting useful?

As discussed, there are more than enough new "entrypoints" for a pentester in an industrial environment, due to the characteristics of industrial IT. Since in many companies the industrial networks are more-and-more connected to the office-networks, weakly protected industrial systems may become a new starting point for hackers. Why attack the fortress at the front, when the weakly protected back door is open? Equipment is old and never designed to be cybersafe, software is outdated and full of buffer overflow leaks, staff unaware of cybersecurity issues? Sounds like hacker-heaven to me.

An industrial pentest is a little like going back in history. Not the newest techniques, hottest tools and programming languages, not Windows 8 etc. but perhaps Windows NT, embedded systems with 64 Kbyte of memory, floppy disks, etc. With the knowledge and tools of today, this yesterday's equipment can be effectively checked for their cybersecurity status. The results are known already: they *are* vulnerable. But most of the industrial IT is so far behind in cybersecurity that any improvement is better than none. Let's get rolling!

ROB HULSEBOS

Rob Hulsebos who lives in the Netherlands is a software-engineer with 25+ years of experience in developing embedded software, machine control software and industrial network technology. He also works as a freelance author for the trade press, reporting monthly on new developments in industrial networks and cybersecurity. In 2010 he assisted Symantec with decoding Stuxnet. Being a software-engineer himself, he knows how easy it is to make a 1-second coding bug keeping hundreds or thousands of security specialists busy for months at a time.

Icon Labs'

Floodgate Defender

Security Appliance for SCADA, industrial, military and other fixed devices

Hardware Specifications

Size: 4" x 4.5" x 1"
 Weight: 13oz
 Operating temp: 0-70C

Using Floodgate Defender

Floodgate Defender can be used to protect any device attached to the Internet or to any TCP/IP network. Floodgate Defender is installed between the device and the Internet and it filters all packets sent to the device. Every packet is compared to the communication policies to determine if it should be allowed and all unauthorized traffic is blocked, stopping cyber-attacks before they even begin.

Installation and configuration

Installation of Floodgate Defender takes just minutes. Simply plug in the Ethernet cable for the device being protecting to Floodgate's A-port and attach an Ethernet cable from Floodgate's B-port into the device. Turn the device on and use the web interface for configuration.

Floodgate Defender provides a secure, easy to use web interface for configuring communication policies.

3636 Westown Parkway
 Suite 203
 West Des Moines, IA 50266
 Ph: +1 515-226-3443
 Fax: +1 877-379-0504
 Email: info@iconlabs.com

www.iconlabs.com

Overview

Floodgate™ Defender is a compact firewall appliance that provides drop in protection for industrial devices. Installation and configuration can be done in minutes, providing instant protection against cyber-attacks from hackers, denial of service attacks, cyber-sabotage attacks, automated hacking bots, and any other Internet-based threat.

A secure web interface allows configuration of customized communication policies. Floodgate Defender enforces these policies, blocking unwanted packets before they are passed to the target device and blocking attacks before a connection is even established.

Hackers Targeting Industrial Devices

Internet-based attacks are on the rise and an increasing number of these attacks are targeting industrial devices. Cyber-criminals, hacking bots, industrial or international espionage agents and even terrorist groups are now targeting industrial, military and utility systems.

Reported attacks against industrial devices include:

- Hackers breached SCADA systems in 3 different cities (based on an FBI report).
 - Pipeline monitoring system that failed due to a DoS attack.
 - Train system delays caused by hackers.
 - Sewage spill caused by a control system that was hacked by an insider.
- Automotive manufacturing plant shutdown resulting from a cyber-attack.
 Pacemakers, insulin pumps and other medical devices hacked by researchers.
 Printers that were hacked for corporate espionage.



Device Protection with Floodgate Defender

Firewall technology is the cornerstone of security for home and corporate networks. Any modern PC includes a firewall. Yet most industrial control devices have no firewall. Worse still, many of these devices have been in service for years and include no security features at all. Replacing or upgrading these systems is often impractical and expensive.

Floodgate Defender allows security to be easily added to existing systems without modifying the network or the control systems. No changes are required to the network and legacy devices do not need to be upgraded. Simply install Floodgate Defender in front of the TCP/IP connection for the device you want to protect, configure the filtering rules, and Floodgate Defender does the rest. With Floodgate Defender you can preserve the investment in your current systems without sacrificing security.

Logging and Alerting

Floodgate Defender can generate an email alert when alarm conditions are detected. Floodgate Defender also maintains a log of all packets that violate the communication policies. These logs can be used for forensic investigation to determine the source of an attack.

Defending Industrial Control Systems with Data Diodes

Originally designed by government organizations to protect top secret information, data diodes are most commonly used in applications requiring the highest level of security such as state secret protection, banking or battlefield up-links.

In recent years I have seen an increasing demand for data diodes in the world of industrial control and automation to protect critical infrastructure due to the simple and virtually impenetrable nature of these devices. In this article we will explore the inner workings and practical control system applications of these unidirectional gateways and provide a step by step guide to creating your own using open source software.

sure the safety of sensitive information within a network. I prefer to call them “Data Diodes” when speaking about Industrial Control and Automation System (Aka ICAS / ICS / SCADA / DCS systems) security because anyone with an electrical background almost instantly recognizes their function. By creating a physical barrier that only allows data transfers in one direction (hence the “uni” in unidirectional) we can enhance security in one of two ways:

What are Data Diodes?

Sometimes known as a unidirectional network or unidirectional security gateway, data diodes en-

- Making a network segment write only (see Figure 1).

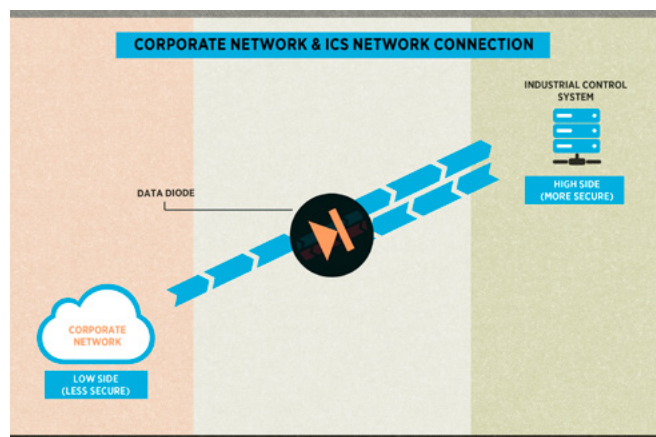


Figure 1. Write Only Control System Data Diode

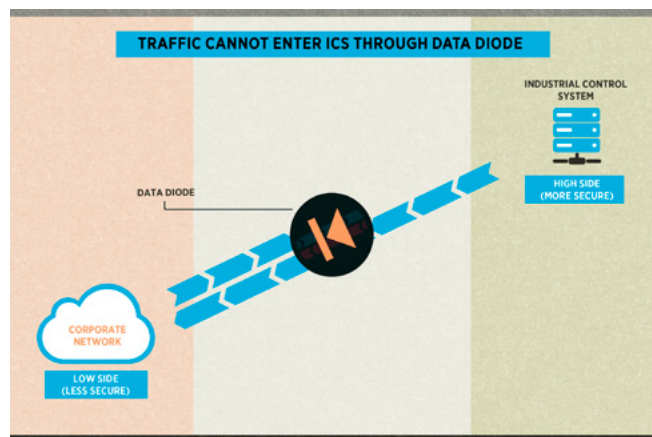


Figure 2. Read Only Control System Data Diode

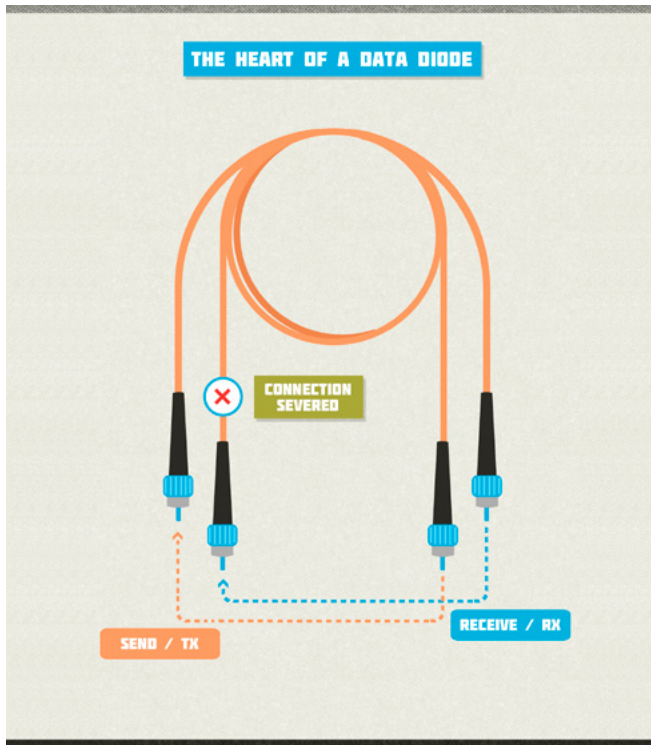


Figure 3. Fiber Optic Patch Cable link at the Heart of a Data Diode

- Making a network segment read only (the more common configuration for control systems), see Figure 2.

Strength in Simplicity

The strength of a Data Diode is its simplicity. At the core of all data diodes is a simple duplex fiber optic connection (fiber optic connections often have a dedicated send / receive fiber strand) with either the send or receive fiber disconnected. Severing one of the physical fiber connections makes it impossible to send data in one direction. (See Figure 3).

What are the Typical Applications of a Data Diode?

Data diodes were originally developed for use in the defense industry in order to protect top secret information from getting into the wrong hands. If you read the marketing materials put out by the data diode vendors you will see they are sprinkled with military terms like “tactical deployment” and “warfighter operations” which is a clear indication of the audience they are targeting. Most data di-

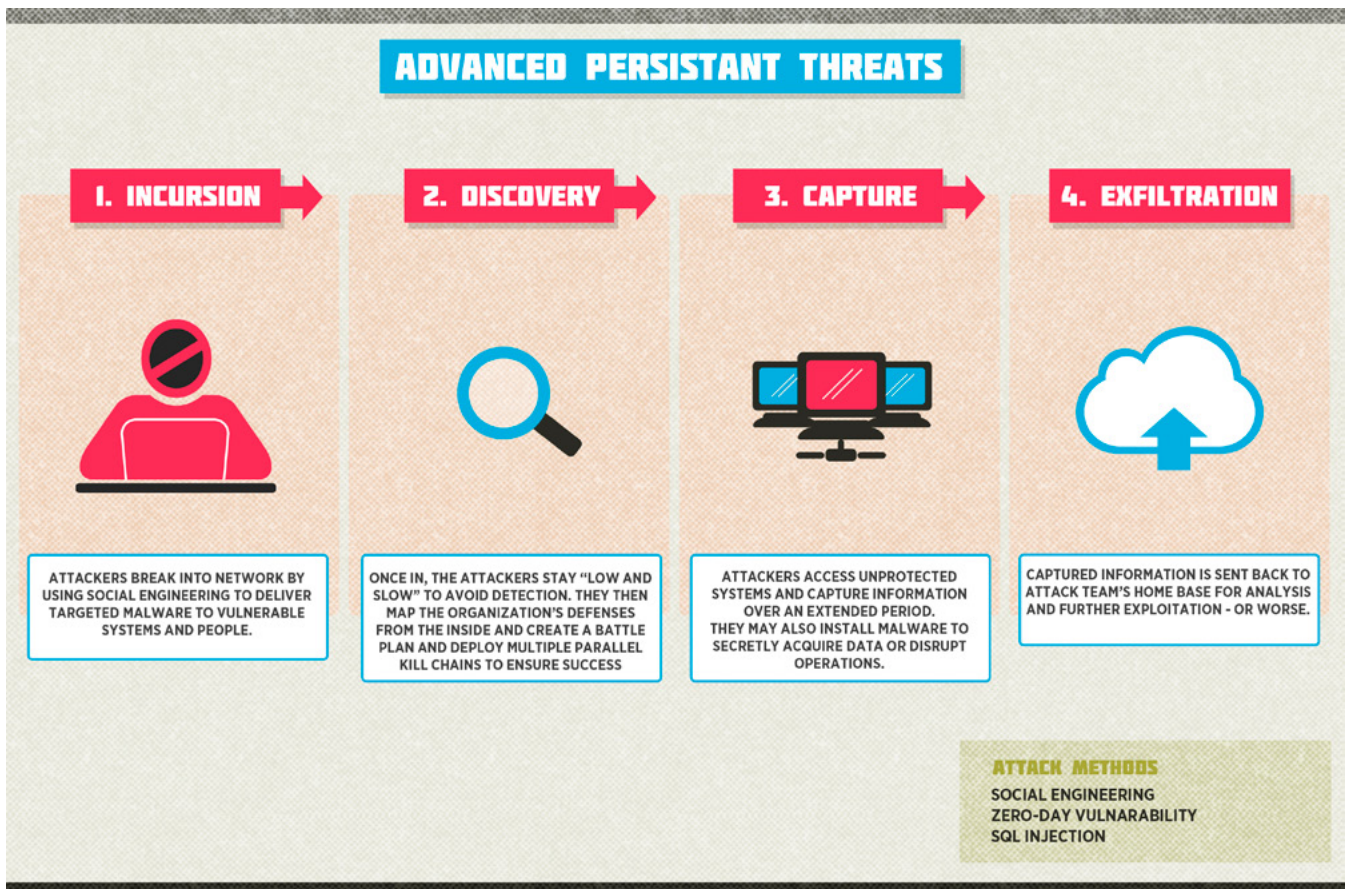


Figure 4. Typical Advanced Persistent Threat

odes on the market today have an impressive array of top level security certificates from countries around the world. Data diodes have been blessed by NERC (North American Electric Reliability Corporation) as a compliant solution for protecting critical infrastructure like power plants. Their ability to securely manage high-traffic systems make them ideal for use in a control system environment. A data diode is an effective defense against data exfiltration (a military term for the covert retrieval of sensitive data) which many Advanced Persistent Threats (APTs) like Flame and the Night Dragon attacks are designed to perform. If the corporate network is unable to send data into the control network, the control network will still be secured if the corporate network is compromised. Also if an industrial control system is compromised by a deep penetrating worm, the hacker will be unable to send commands or updates because of the one way network traffic gateway. (See Figure 4).

ICSSEC (Industrial Control System and Automation System Security) in the Real World

If you believe in the so called control system “Air Gap” then I have a unicorn farm run by leprechauns I would love to sell you. I will not dispute the fact that it is a terrible idea to directly connect any piece of industrial equipment or SCADA system to the Internet. However, in my experience most control systems are indirectly connected to the Internet. Why would anyone be foolish enough to indirectly connect a SCADA / DCS system to the Internet? The answer is simple, people need the data. The data generated by an industrial control system is pure gold; far too valuable to not be connected to the corporate network. Data taken directly from the SCADA / DCS is used by most business units in an organization, for example:

- Accounting
 - How many widgets did we produce?
 - How much oil did we pump?
 - How much process downtime did we have?
- Regulatory Compliance
 - How much greenhouse gas did our process produce?
 - Did the formula change for the drug we are manufacturing?
- Health and Safety
 - For the past 15 years has the toxic gas our workers have been exposed to been within a safe limit?
- Preventative Maintenance
 - How many running hours until we need to rebuild that motor?
- Process Optimization
 - What are the most common alarms?
 - How long does it take the operator to intervene in the SCADA system when the process enters an abnormal situation?
 - What was the energy usage in DCS A compared to DCS B?
- Quality Control
 - Was there a problem with the process while we were making the product with serial #192813?

Keep in mind that many control systems are in remote locations, far from the corporate headquarters that pay their bills. Most people are not willing to jump on a plane to collect some data

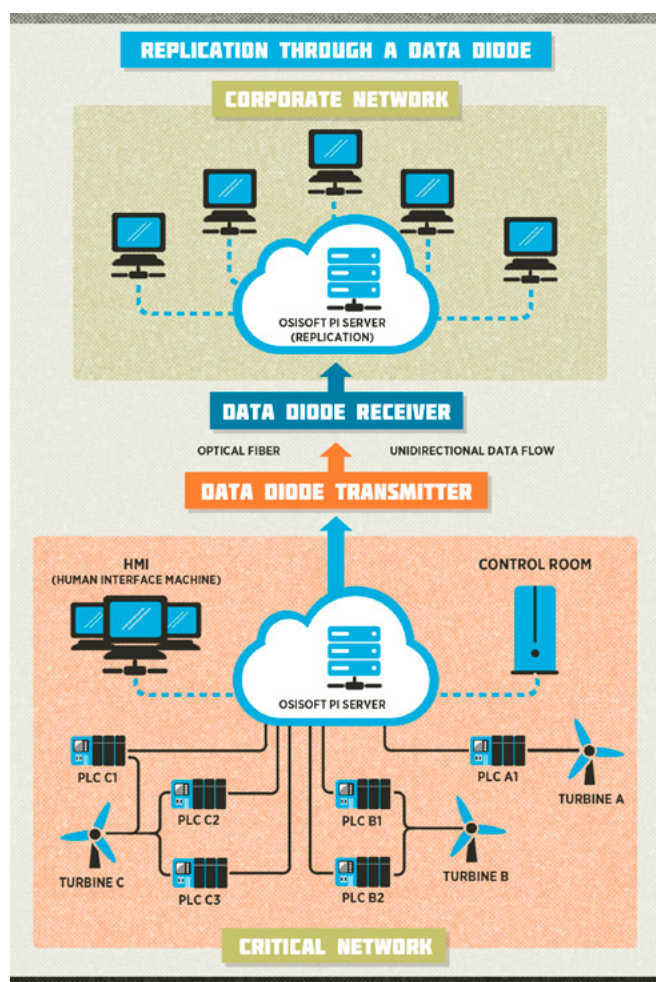


Figure 5. Database Replication through a Data Diode

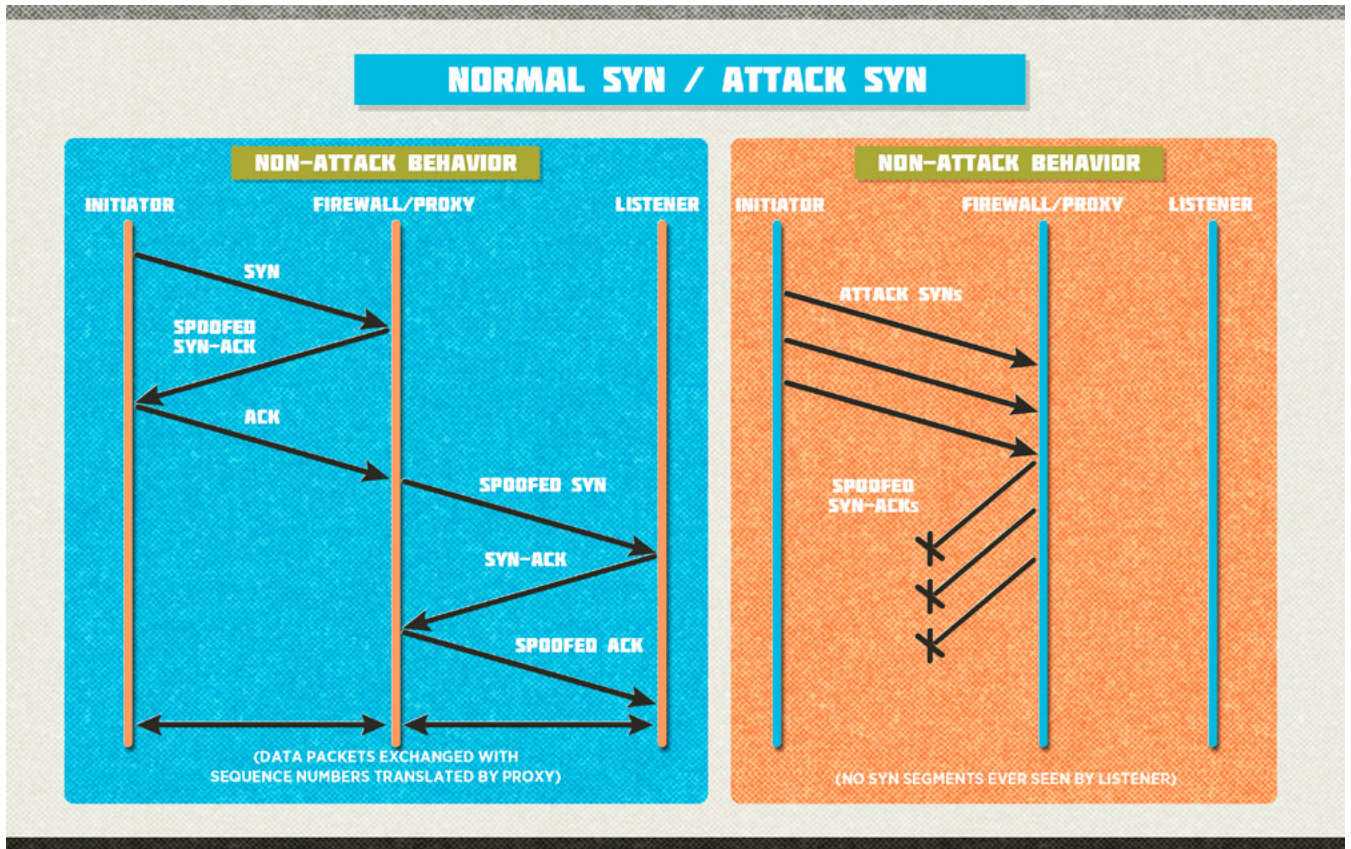


Figure 6. TCP SYN ACK Two Way Communication

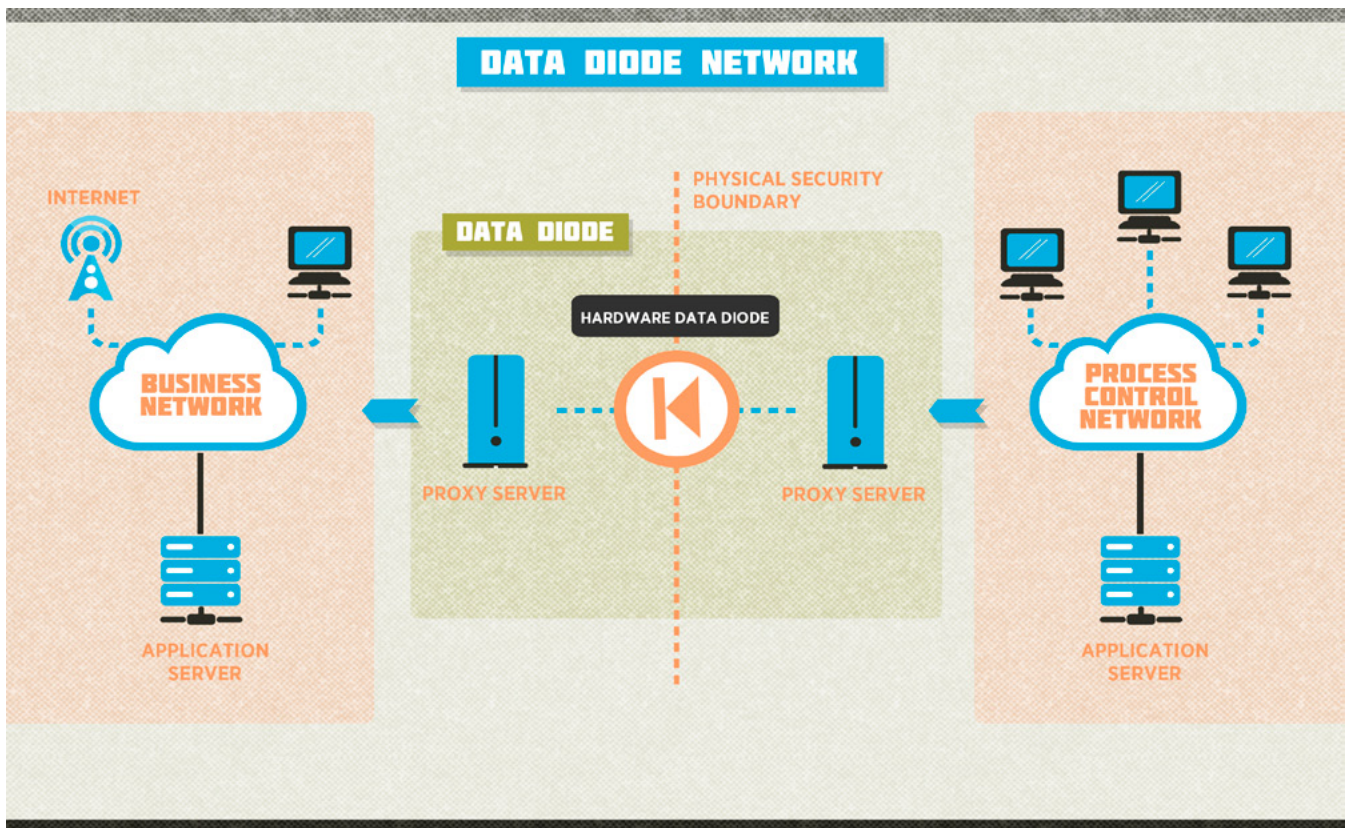


Figure 7. Data Diode Reverse Proxy Servers

they need for a report and reading values over the phone is very error prone. The Internet is the most cost effective way to transmitting data over long distances. Often the bridge between the corporate network and the industrial control network is a gateway computer, a firewall or a series of firewalls. Firewalls rely on many layers of software to segment a network. Due to the nature of software a small oversight in the real-time OS, rule engine, configuration or installation could allow an attacker to bypass the Firewall completely. ICSsec (Industrial Control System and Automation System Security) guidelines suggest that firewalls from multiple vendors should be used in case one vendors firewall is compromised (NIST 800-82, IEC 62443 formerly ANSI/ISA99). Firewalls certainly play an important role in any control system's Defense in Depth (DiD) strategy, but it is important to remember that history has shown us that they are not impenetrable. If you are only interested in ac-

cessing the valuable information that a control system is producing, than a data diode is a more secure choice. You are providing read access to the data in the ICS without allowing anyone to write data to the ICS. A typical example is transferring data from one SQL server in your ICS to another SQL server in your corporate network. If the corporate network is compromised there is no physical way data can be sent to the control network. (See Figure 5).

The Problem with One Way Data

If you are familiar with TCP/IP (Transmission Control Protocol), you are probably questioning the practicality of such a solution as TCP/IP requires two way communication to work. TCP/IP requires a two way handshake (SYN / ACK) in order to establish a connection and terminate a connection. In fact there is a very common misconception that it is impossible to use TCP/IP connections through a data diode. (See Figure 6).

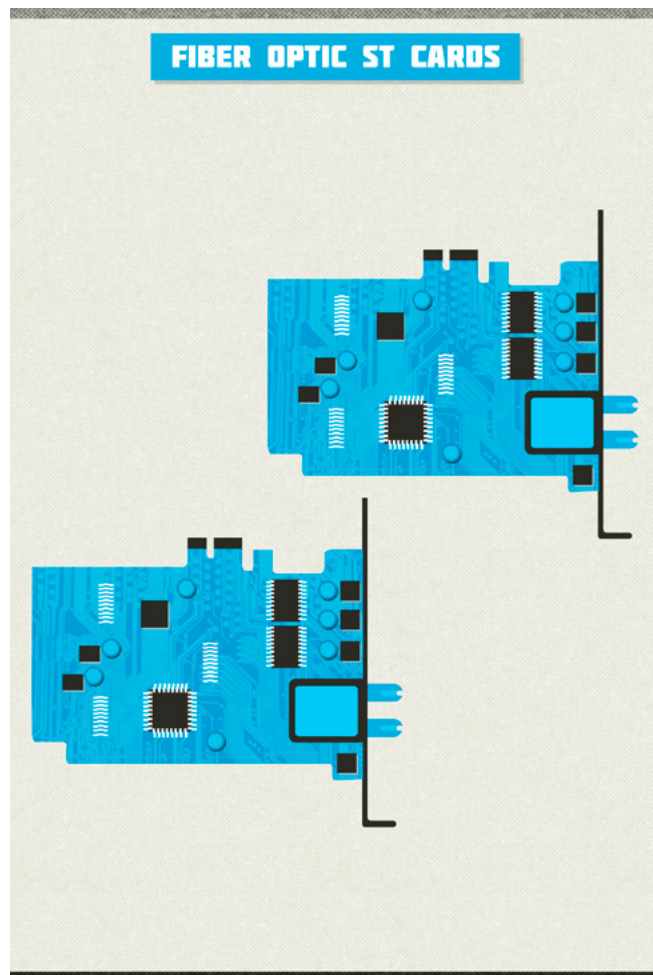
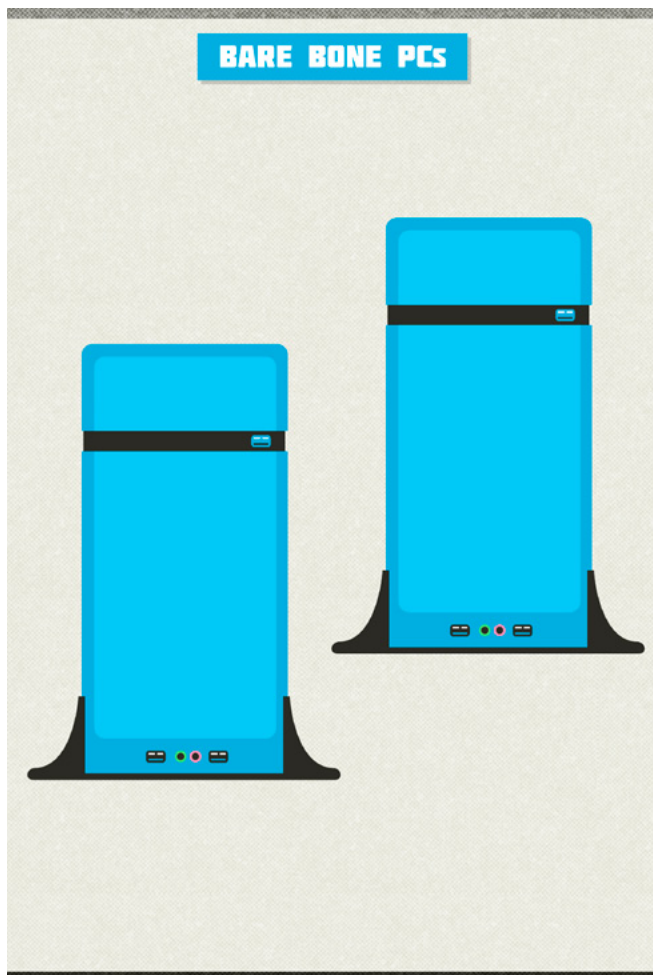


Figure 8. Two Bare Bone Mini-PCs for our homemade data diode

Figure 9. Two PCI Express Fiber Optic ST Cards for the Fiber Optic Link in our do-it-yourself Data Diode

There are two ways around this problem:

- UDP (User Datagram Protocol) variants of protocols should be used when available. UDP is a lightweight protocol typically used for speed as it does not waste network bandwidth by handshaking or data integrity checksums.
- TCP/IP client-server reverse proxies on either end of the data diode can be setup to respond to the hand shaking requests automatically without the need to actually send any data back to the insecure network. A reverse proxy server retrieves data from another computer and serves it up as if it were the original source. Reverse proxies are most frequently used to speed up the delivery of web content and reduce the load on the content main server. The client-server proxies solution should work in most cases however, thorough testing should be completed in

a lab environment before deploying a data diode solution into an ICS. (See Figure 7).

How to Roll Your Own Data Diode

If you were to crack open a typical data diode you will see it is simply made up of two mini-pcs with a fiber-optic link running between them. There are dozens of patents around variants of data diodes and data diode software. For example there is a patent for a data diode that only uses a single computer to handle both ends of the connection (which seems less secure to me). A fiber link between two computers is far too simple a concept to patent, so you won't end up in court creating a data diode in this configuration. Now let's step through the process of creating our own data diode.

Step 1. Purchase two computers

It is important to find a small form factor computer which supports a PCI-Express card for our two fiber optic PCI-Express cards (reverse) proxy servers. For most industrial applications I would purchase a couple of fan-less industrial PCs with solid state hard drives that can be stored in a locked computer panel box or server room.

For the purposes of our proof of concept I will purchase two low cost PCs:

- Slim Bare bones PC with a PCI-Express card slot
- Solid State Hard Disk drive
- 2 Gigs memory
- i5 Processor

These PCs should come with an integrated Ethernet card which we will plug our network connection through.

2 x – Barebones PC with PCI-Express card slot – \$600.00 each (see Figure 8).

Step 2.

Purchase two fiber optic PCI-Express cards

If you don't have experience with fiber optic networks you need to be aware of the many standards and modes that are available. It is critical that you select fiber optic cards and a patch cable that are all compatible.

I have selected multi-mode "Fiber-to-the-desk" PCI-Express card with ST connectors which make it very easy to disconnect one of the fiber links.

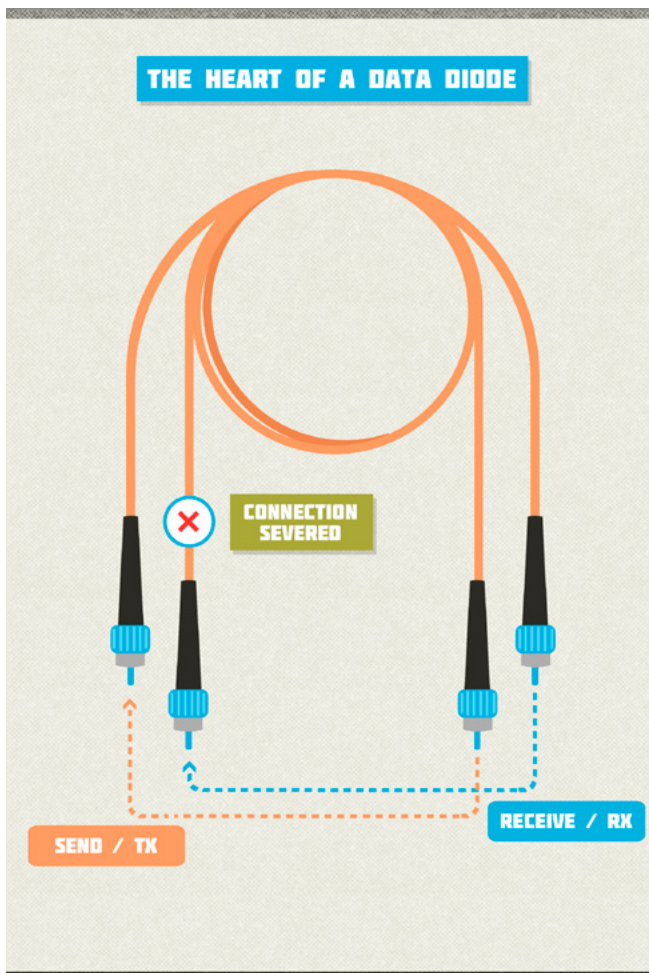


Figure 10. The heart of our handcrafted unidirectional gateway is the ST Fiber Optic Patch cable

2 x – Gigabit Ethernet Multi-Mode ST Fiber Card 1000Mbps PCI-Express – \$200.00 each (see Figure 9).

Step 3. Purchase a fiber optic patch cable

I have found a suitable multi-mode fiber patch cord with male connectors on each end:

3m Multi-Mode 62.5/125 Duplex Fiber Patch Cable ST – ST – \$12.00 (see Figure 10).

Step 4. Install a Secure Operating System on the PCs

I prefer to use OpenBSD because it is free, open source, Ultra-secure out of the box and I have friends here in Calgary who are OpenBSD gurus.

Step 5. Configure your Reverse Proxy

Depending on the data you want to replicate you can either configure an open source reverse proxy like nginx (engine x) and use your database’s web services to replicate the data.

Step 6. Disconnect one of the fiber optic ST connectors

Once you have your two proxy servers configured and communicating to each other you can simply disconnect one of the two fiber ST connectors. You will likely need to spend time properly configuring your reverse proxy servers to relay the information correctly and you will need to write some scripts in your database to perform the continuous data replication. (See Figure 11).

For a total cost of \$1612 and some tender loving coding, you too can have your own home-brew Data Diode!

Conclusion

Data Diodes represent a simple yet virtually impenetrable way of segmenting a network. They have been used for years to secure classified information by government organizations and are an excellent complement to firewalls in a typical control system’s defense in depth strategy. Adding a data diode to your network doesn’t have to cost tens of thousands of dollars either. You can reap the benefits of a unidirectional data diode for a few thousand dollars and some technical elbow grease.

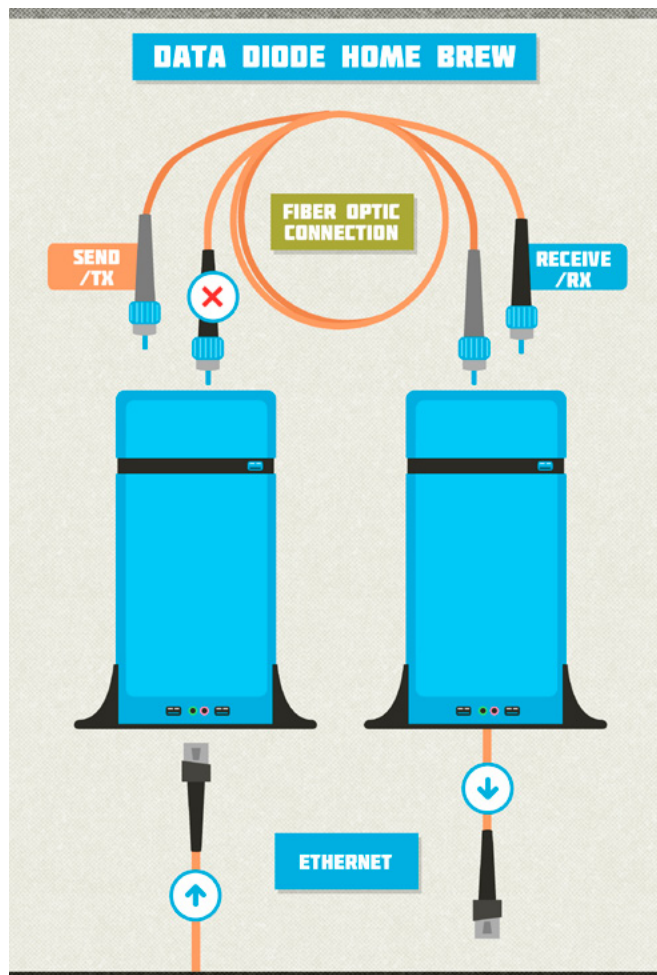


Figure 11. Our completed home brew data diode configuration

AUSTIN SCOTT

Austin Scott is CEO of Synergist SCADA Inc and heads up a talented team that offers a consummate blend of controls expertise, industry know-how, and advanced software development skills. “Synergist SCADA Inc. is focused on maximizing the effectiveness of our customers’ SCADA investment. We provide control systems design, upgrade strategies, HMI / SCADA / PLC programming, security audits, and field services.” Austin Scott is currently authoring a book on pragmatic ICS Security practices that is due out this summer.



Allow
us to
guide
your
CAREER



SENIOR
PRACTITIONER



2013 PUBLIC COURSE SCHEDULE

CISMP

Mar 18-22, Apr 22-26, May 13-17, Jun 10-14,
Jul 8-12, Sep 30 - Oct 4, Oct 14-18, Nov 18-22

PCiBCM

Mar 18-22, Apr 8-12, Apr 22-26, Jun 10-14, Jul 8-12,
Aug 5-9, Sep 16 -20, Oct 14-18, Nov 11-15, Dec 9-13

PCiIRM

Apr 22-26, May 6-10, May 20-24, Jun 3-7, Jun 17-21,
Jul 8-12, Jul 22-26, Aug 5-9, Oct 7-11, Oct 21-25, Nov 4-8,
Nov 18-22, Dec 2-6, Dec 16-20

If you are interested in learning more, get in touch:
contact@infosecskills.com.



PRACTITIONER

SCADA

Device Security – Threats, Hackers and How to Protect Against Them

For many decades, Supervisory Control and Data Acquisition (SCADA) systems have played a very important role in controlling many of the critical infrastructure systems that our modern society depends upon. These have included building controls, electrical power distribution, elevators, hydroelectric dams, natural gas and oil pipelines, traffic lights, train switching systems, water treatment facilities and many others.

Understandably, security for SCADA systems is a high priority because of its critical role in controlling these crucial systems. What makes this issue so critical is the fact that many legacy SCADA devices that were originally designed many years ago without security measures are now being connected to the Internet. In most cases, these devices also lack the ability to detect and report traffic abnormalities, probes or attacks, or to manage and control security policies. While newer systems may include improved security, many SCADA devices remain deployed for 10 years or more, often in remote areas or with difficult access, resulting in very slow turnover to newer, more secure devices.

In addition to system level security issues, SCADA protocols themselves are often inherently insecure. They may lack basic security measures. Instead they often rely on “security by obscurity” or on isolation from public networks for security. Without security measures such as authentication and encryption, the underlying protocols provide an easy avenue for hackers wishing to attack SCADA devices.

SCADA Networks

SCADA systems are often complex networks with multiple components. These systems may be

fully automated where all control is handled by computers, fully manual in where control is performed by human operators, or a hybrid system where some control is performed automatically and some is performed by human operators. To perform all of these functions, many SCADA systems include:

- Control computers – Embedded computers or dedicated PCs receiving information from the sensor networks, reporting this information to the management systems, and controlling the associated operating equipment. These computers may make decisions automatically based on the information derived from sensors, or may relay commands received from management computers.
- Management computers – Computer terminals with an HMI (Human Machine Interface) connected to the SCADA network. These computers provide an interface for operators to monitor and control the devices on the SCADA network.
- Networked communication (local and remote) – SCADA networks use a variety of communication technologies. Serial communication, USB or proprietary wired networks are used for short range communication. Ethernet, TCP/IP,

Wi-Fi, dial-up networking, cellular packet data and other methods are used for long range communication. Increasingly, SCADA networks utilize the Internet for long range communications and remote access.

- Field Interface Devices – Sensors detecting and reporting power levels, flow rates, temperature, pressure, and local control devices such as motor controls, valve actuators and control switchboxes.
- Operating equipment – Motors, pumps, automated factory systems, and valves controlled by the SCADA network.
- Interconnection to business process systems – Frequently, SCADA networks are connected to corporate networks to allow them to interconnect with business process systems.

SCADA networks may contain a mix of PCs and special purpose embedded systems running a real-time operating system such as INTEGRITY, MQX or VxWorks. Frequently, the control PCs used in SCADA networks were installed when the system was first deployed and have not been updated with newer operating system versions or software patches for improved resistance to attacks. As a result they are often very vulnerable to attack. Most embedded computers in SCADA networks were designed before security was a major concern and contain few, if any, security measures.

In many cases, the PCs within the SCADA network can be protected by ensuring they are running a current operating system with the latest security patches and security software. In some cases, the PCs are running SCADA specific software that is only supported on an older OS version preventing the PC from being upgraded. In other cases PCs cannot be upgraded because the cost of retesting to achieve required certification compliance is prohibitive. Running old, unpatched OS versions creates security issues. In the case of these legacy PC systems, and for embedded SCADA computers, another way of adding security without modifying the device is required.

Attacks on SCADA Networks

There is little dispute that additional protection is needed for SCADA networks. The FBI recently acknowledged that hackers gained access to SCADA systems in 3 different US cities. Other reported attacks on SCADA systems include:

- Train system delays caused by hackers
- Sewage system spillage caused by a disgruntled former employee
- Automotive manufacturing plant shutdown resulting from a cyber-attack

Given the large number of deployed SCADA devices and the slow turnover to modern and secure SCADA devices, the SCADA marketplace urgently needs the ability to add security to both existing legacy devices and to new designs in a cost effective manner.

Even SCADA devices located behind a corporate firewall should still be protected by a SCADA firewall. The security requirements for SCADA devices are typically different than for the corporate network as a whole. The SCADA firewall can be configured with communication policies that are more restrictive than those supported by the corporate firewall and that are customized for the individual device, rather than for the entire network. In addition, a SCADA firewall can be used to protect from insider attacks or attacks originating from within the corporate network. PCs located on corporate networks typically include an end point firewall to implement an additional layer of security. SCADA devices should be afforded the same level of protection.

SCADA Security Requirements

A SCADA security solution must provide the ability to control communications, detect and report attacks or suspicious traffic patterns, and to allow centralized control of security policies. These capabilities would provide SCADA devices with a much higher level of security and protect them from the majority of cyber-attacks.

The SCADA firewall must provide:

- Control of the packets processed by the device
- Protection from hackers and cyber-attacks which may be launched from the Internet, inside the corporate network, or WiFi networks
- Protection from DoS attacks and packet floods
- Ability to detect and report traffic abnormalities, probes or attacks.
- Ability to manage and control changes to filtering policies

One option is a low cost, SCADA aware firewall appliance that can provide these capabilities. Unlike enterprise firewalls protecting all of the com-

puters on a corporate network, a SCADA firewall protects just a single device. Since the firewall is only filtering traffic for a single device, it does not need to perform any routing functions and can be customized specifically for the requirements of protecting a specific SCADA device. It only requires two Ethernet ports and can be implemented on low cost hardware, providing a customized and yet cost effective solution. This kind of “bump in the wire” device is simply plugged into the network in front of the SCADA device, inserting a layer of protection.

SCADA Firewalls vs. Desktop Firewalls

Firewall technology is standard in home and corporate networks and is a proven and reliable technology. So why not just use one of these existing solutions to create a SCADA firewall? For the same reasons desktop operating systems are not used in embedded devices; they are slow, big, and are not easily ported to a low cost, special purpose device. To build a SCADA firewall requires a small, low cost solution that will work on inexpensive hardware. In addition, the solu-

tion must be customizable to support filtering of SCADA protocols.

Other Features of a SCADA Firewall

In addition to providing filtering, there are a number of important requirements for a SCADA firewall. It is crucial to provide users with a flexible and easy to use, yet secure, configuration interface. If the firewall configuration can be compromised, then the firewall can be reconfigured and bypassed, or possibly even disabled.

The firewall should also provide statistics, logging and reporting capability to allow security audits to determine if the device has been attacked, what IP address the attack originated from, and other relevant details. Integration with a management system to allow centralized policy management and configuration is also critical for large scale deployments (see Figure 1).

The “Bump in the Wire” SCADA firewall can be used to protect devices located at remote locations without making any modifications to the SCADA device. It can also be used to protect SCADA devices located on a factory floor or other non-remote location. For new SCADA devices, the firewall software can be integrated into the device itself to ensure protection.

Blocking Attacks with a SCADA Firewall Using a VCN – Virtual Closed Network

As stated above, many of these SCADA devices with limited security are now connected to the Internet, exposing their security vulnerabilities. This can be remedied by using a SCADA firewall to create a virtual closed network (VCN).

To create a VCN, the designer needs to define the communications policies for the device, restricting communication to only what is required. The communication policies define who the device is allowed to talk to, what protocols are allowed, and what ports are open. The defined communications policies are then encoded as firewall rules. The firewall filters messages before the device processes the messages. By enforcing the rules, the firewall only allows communication with known, trusted devices, creating a virtual closed network.

In a system without a firewall, a hacker may attempt to remotely access the device using default passwords, dictionary attacks, or stolen passwords. Such attacks are often automated, allowing a huge number of attempts to break the sys-

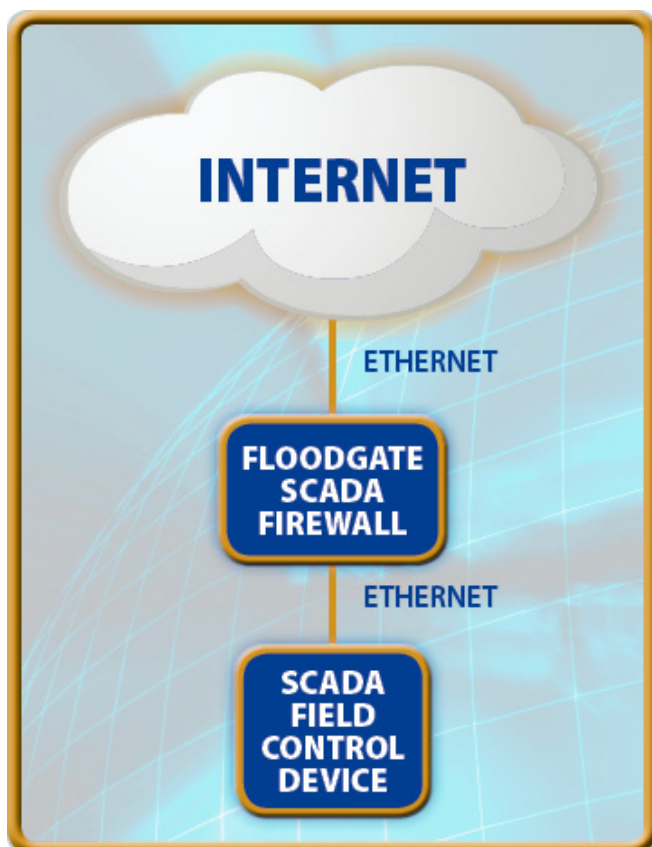


Figure 1. A firewall to protect SCADA devices can be implemented as an external “Bump In The Wire” firewall that protects the SCADA device from Internet delivered threats

tem's password. With a VCN, the same system is protected by a firewall configured with a whitelist of trusted hosts. The firewall's filters will block attacks from the hacker before a login is even attempted because the IP or MAC address is not in the whitelist of trusted hosts, thereby blocking the attack before it even really begins.

SCADA Firewall Design

The main requirement of a SCADA firewall is to filter network traffic and control who the SCADA device talks (IP and MAC address filtering) to and what communication is allowed (port and protocol filtering). Ideally, the firewall would also provide event reporting, integration with a management

system, and protection from Denial of Service and other cyber-attacks. Event reporting and integration with a management system provide visibility into abnormal network traffic, alerts in the event of a cyber-attack, and centralized control of security policies.

The firewall must also provide the ability to configure communication policies, a set of rules specifying which packets are processed and which are blocked. Rules can be set up to block or allow packets by IP address, port, protocol, or other criteria. Some firewalls support advanced rules allowing additional fine-grained control over the filtering process.

A SCADA firewall may also provide Stateful Packet Inspection (SPI) and threshold-based filtering. SPI filtering maintains information on the state of the connection and uses that information to distinguish legitimate from malicious packets. Threshold-based filtering maintains statistics on the number of packets received in order to detect and block packet flood DoS attacks. Undetected and unblocked DoS attacks may overload the SCADA device, degrading its performance or causing it fail altogether.

Many attacks are blocked before a connection is even established because each packet received by the devices must pass through the firewall for filtering before being processed. This provides a simple, yet effective layer of protection that is currently missing from most SCADA devices (see Figure 2).

Filtering options for TCP/IP and ProfiNET

As stated earlier, it is critical to protect SCADA devices that are connected to the Internet or a corporate network, from cyber-attacks that could originate from the Internet or even from insiders on the corporate network. Many SCADA protocols now have variations that run over Ethernet or TCP/IP. Modbus can run over TCP/IP and ProfiNET is a standard for Profibus over Ethernet. To protect these devices the SCADA firewall must be able to filter both Ethernet and TCP/IP traffic.

There are three main types of filtering a firewall can perform.

- Static filtering or rules-based filtering: Compares each packet to a set of rules to determine if the packet should be blocked or allowed. All decisions are made based on the information in the packet.

Floodgate Operation

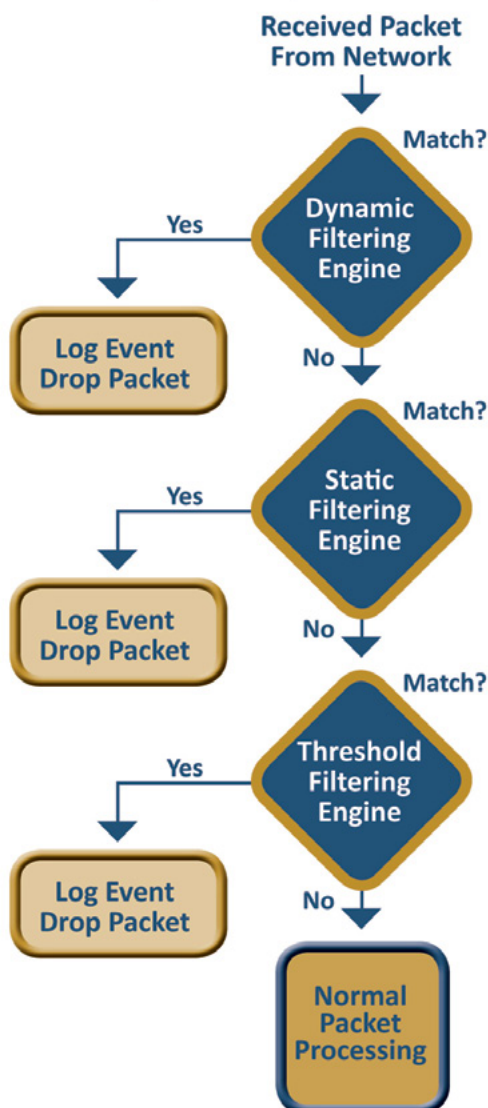


Figure 2. A multi-stage filtering engine provides fine-grained control over the packets processed by the SCADA device

- Stateful packet inspection or dynamic filtering: Maintains information on the state of each connection (dynamic information) and uses the information to make filtering decisions.
- Threshold-based filtering: Keeps statistics on packets received and monitors for threshold crossings to detect packet floods and Denial of Service (DoS) attacks.

Selecting a Filtering Option

Static, or rules-based filtering, provides a simple and effective tool to enforce closed communication and, for some devices is the only filtering needed. With rules based filtering, any communication from a non-trusted IP or MAC address, or to a closed port or protocol, will be blocked, isolating the device from attack (Figure 3).

If rules-based filtering does not provide sufficient protection, then Stateful Packet Inspection (SPI) or threshold-based filtering may be added for additional protection. Stateful packet inspection provides protection against packets received with invalid TCP state information, a common Internet-based attack.

Threshold-based filtering is complex and requires significant system processing time and memory, but provides a powerful tool for detecting packet floods and DoS attacks.

Static Filtering/ Rules-based Filtering

Static filtering works by allowing a set of rules to be configured specifying the filtering field (IP or MAC address, protocol number, port value, etc.), the filtering type (whitelist vs. blacklist), and the values

to be matched. A whitelist is a list of allowed values. If a packet is received and the value is on the list, it is allowed. If not, it is blocked. A blacklist is the opposite, any values on the list are blocked and all other values are allowed.

For example, a rule set could look like the following:

- Rule 1, WHITELIST, IP source address, {192.168.0.0 – 192.168.0.255}
- Rule 2, WHITELIST, IP protocol, {1,2,6,17}
- Rule 3, BLACKLIST, UDP destination port, {700-799}

Static filtering requires the ability to specify the rules set and a filtering engine to evaluate each packet against the configured rules. With the rules show in this example, the filtering engine first checks the IP address of each packet. If the IP source address is not in the range of 192.168.0.1 – 192.168.0.255, the packet will be blocked. Otherwise the filtering engine will proceed to the next rule.

The second rule specifies that the IP protocols of ICMP, IGMP, TCP and UDP (protocol numbers 1, 2, 6 and 17) are allowed. Packets received with

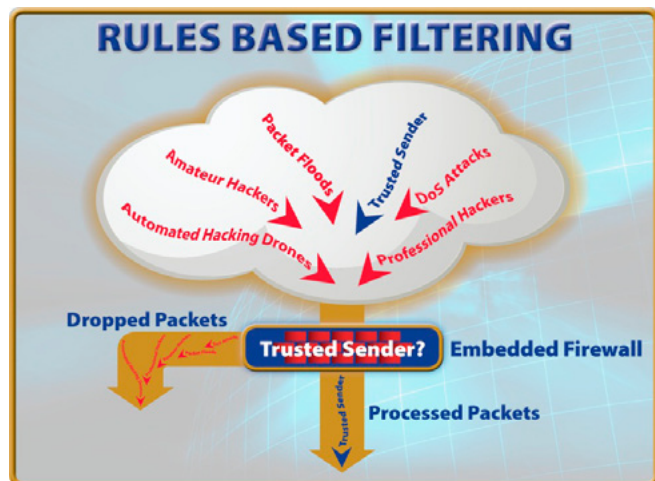


Figure 3. Rules-based filtering is used to enforce communication policies, blocking packets from non-trusted senders, and isolating SCADA devices from attack

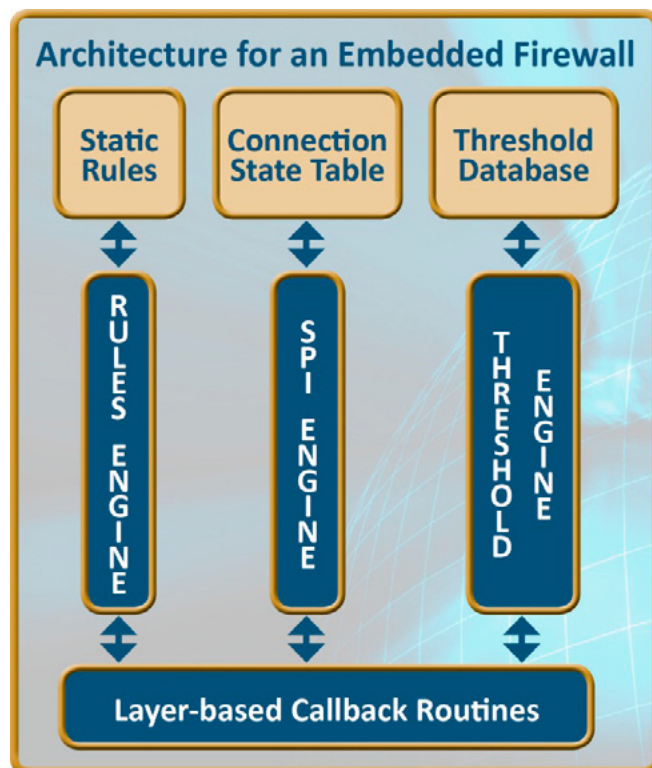


Figure 4. Combining SPI filtering, rules-based filtering and threshold filtering provides a SCADA device with a robust, multi-layered defense against cyber-attacks

any other protocol value will be blocked, even if it is from a whitelisted IP address. The third rule specifies that UDP ports 700-799 are blacklisted. Any UDP packets received for these ports are blocked.

Stateful Packet Inspection (SPI)

SPI maintains information on the state of each connection and uses it to make filtering decisions. Connection oriented protocols such as TCP use the protocol connection state. In contrast, for connectionless protocols such as UDP, the connection state is either CLOSED or ESTABLISHED based on how recently a packet was sent or received for a given IP address and UDP port.

This requires a “state table” which is updated as connections are established, proceed through the connection states, and closed. As packets are received the firewall validates them based on the current state of the connection and then updates the state table as needed. SPI is protocol specific and therefore the SPI engine must implement a state transition and state validation routine for each supported protocol.

Threshold-based Filtering

Threshold-based filtering works by collecting and maintaining statistics on the packets received and monitoring for threshold crossings based on configured time intervals and threshold levels. If the number of packets received from a specific IP address during any time interval exceeds the configured high-water threshold, future packets from that IP address will be blocked. Once the traffic from that IP address falls below the configured low-water threshold, the filter is turned off and packets from that IP address are again allowed. Implementing threshold-based filtering requires a

References

- Source: John Gantz, The Embedded Internet: Methodology and Findings, IDC, January 2009.
- Source: Cui, Song, Phatap and Stolfo, Brave New World: Pervasive Insecurity of Embedded Network Devices, Intrusion Detection Systems Lab, Columbia University
- www.synergistscada.com/the-top-5-scada-security-threats-for-2012/

database to maintain packet counts and a monitoring module to detect and enforce threshold crossings.

Summary

Firewalls provide a simple and effective layer of security and have long been used to protect home and enterprise networks. A small, SCADA aware firewall can be used to protect devices in SCADA devices from a wide range of cyber-attacks. By controlling who the SCADA device talks to, most attacks can be blocked before a connection is even established. A cost effective SCADA aware firewall appliance can provide a critical layer of defense for legacy SCADA devices, and a software based SCADA firewall can be integrated into new devices, ensuring security is part of the device.

Icon Laboratories, Inc.

Icon Labs is a leading provider of embedded networking and security solutions. Icon Labs’ award-winning software is at work every day, in broadband Internet access devices to core network routers, from smart modems to optical cross-connects, and from the factory floor to the operating room. Founded in 1992, Icon Labs is headquartered in West Des Moines, Iowa. For more information, visit www.iconlabs.com, send email to info@iconlabs.com, or call 1.888.235.3443 (U.S. and Canada) or 515.226.3443 (International).



ALAN GRAU



Alan Grau is President and co-founder of Icon Labs, a leading provider of security software for embedded devices. He is the architect of Icon Labs’ award winning Floodgate Firewall. Alan has 20 years of embedded software experience. Prior to founding Icon Labs he worked for AT&T Bell Labs and Motorola. Alan has an MS in computer science from Northwestern University.

Alan has an MS in computer science from Northwestern University.

Interview with

Dan Brabec

Business Manager of SCADA Products at
Motorola Solutions

Dan's studies have included chemistry, environmental chemistry and applied research in water quality, among others. At Motorola, Dan has held a variety of positions associated with Motorola's fixed data and SCADA products.

PenTest: Hello Dan, could you share some background on Motorola's achievements in the field of Industrial Control Systems?

Dan Brabec: Motorola has been a provider of SCADA solutions for over 40 years. We have been a pioneer in the intelligent use of radio for control systems. The current generation products available now are the Motorola ACE3600 Remote Terminal Units (RTUs). They are a modular mid- to high-tier SCADA solution using Motorola analog and digital radio systems such as ASTRO, TETRA and MOTOTRBO (as well as other communication means). Motorola SCADA solutions serve many traditional Integrated Control Systems (ICSs) such as Water, Waste Water, Oil & Gas and Electric Power distribution. Motorola SCADA solutions are also widely deployed in public safety applications such as Early Warning Systems and Fire Station Alerting.

PT: So, now that we know that SCADA systems are being used in most of the critical industries like Energy, Communication and Military. What are the Threats that these systems face?

DB: Threats to SCADA systems can be divided into two main categories: directed threats such as sabotage and terrorist attacks, and indirect threats like operational errors and viruses.



MOVE TOMORROW'S BUSINESS TO THE CLOUD TODAY

In most SCADA systems, field devices like our RTUs are located in remote un-manned sites. The main threats for those field devices are: unauthorized access, malicious compromise of the device, as well as using the communications network for unidentified actions such as spoofing, resource exhaustion or replay attacks. The potential outcomes from any of these actions include: breakdown of the critical infrastructure, lack of system availability, damage to equipment, data loss, personal safety issues, and ultimately revenue loss and possible penalties.

PT: Even though, the security posture depends on the overall environment, what are the kinds of proactive security measures have been built into Motorola's SCADA Systems?

DB: Security methods effectively used in other critical networks have now been applied to secure Motorola SCADA. The most important features in the new enhanced security ACE3600 systems now include:

- SECURITY POLICY ENFORCEMENT – System-wide set of security settings defined and installed in all equipment.
- BUILT-IN FIREWALL – Filters IP communications by port, direction, protocol and IP address.
- ACCESS CONTROL – User authentication tools to verify specific user access and determine if use is legitimate and allowed. It is executed at the RTUs (M2M) or system servers.
- ROLE-BASED ACCESS CONTROL – Restricts types of access to authorized users only. The system administrator can define job roles and assign different combinations of permissions to each role.
- INTRUSION DETECTION SYSTEM – Legitimate traffic is allowed but unauthorized access activities, such as an attempt to alter an RTU program or add unauthorized data packets, are identified. ACE3600 blocks these activities, logs the events and if enabled sends a report to the system administrator.
- APPLICATION CONTROL SOFTWARE – Also known as “white listing”, this software blocks unauthorized applications and code on PCs and RTUs. ACE3600 firmware protects user programs with this technique, and ACE3600 configuration management tools (STS) on PCs are protected with McAfee™ Solidifier.

YOUR TRUSTED ADVISOR
ON CLOUD COMPUTING

MULTI-VENDOR
ANY DEVICE
HYBRID CLOUD



- **ENCRYPTION** – An algorithm makes our data readable only by a device with a specific key to decrypt the message. ACE3600 communication data encryption prevents listening in or spoofing a message. Data stored in the ACE3600 is also encrypted using an AES (Advanced Encryption Standard) with a 256-bit, FIPS-140-2 approved key.
- **UNUSED PORT DEACTIVATION** – A mechanism to disable communication in any ports that are not used.
- **TIME-WINDOW COMMANDS** – Adds an additional layer of defense via the application that designates a “time window” of action in response to a command message.

PT: What was, in your opinion, the root cause that led to the Famous Stuxnet Episode to be successful?

DB: In my opinion, Stuxnet was a very sophisticated worm that was developed purposely to target specific operations of a particular control vendors products. All the signs point to a very high level of knowledge and effort and it seems to have been at least partially successful. I assume a long time will pass before we learn all the details behind the how and why of Stuxnet and it would be inappropriate to speculate any further.

On the other hand, Stuxnet was very innovative in the way it exploited both IT and SCADA system vulnerabilities, in the way it penetrated into systems that were “detached” from the outside world and in the way it operated on the targeted systems without revealing itself.

PT: How can we safeguard our industrial control systems, where SCADA is the underlying Mechanism, from Stuxnet like State backed attacks?

DB: The main safeguard is awareness and prevention of the various cyber treats and risks. This can be accomplished by using existing solutions such as those offered by Motorola, and by using methodologies recommended by ICS-CERT, NERC and other agencies.

PT: What kind of change of perspective have you seen from your clients about securing their SCADA infrastructure post Stuxnet?

DB: Stuxnet has made an impact by alerting the concern and viewpoints of our higher level exist-

ing and potential clients, but this has not translated into as much action as one would have hoped. We see more interest in other parts of the world compared to the United States at this time.

PT: To what extent does Motorola help its Clients in securing their SCADA infrastructure?

DB: We counsel our clients on the importance of securing their systems and offer services to help analyze their networks and make recommendations as to how to improve their security.

PT: Do you find it challenging to find the right talent to help the clients designing and running a secured SCADA system?

DB: Not particularly. Motorola has been involved with security for a variety of governmental and military communication systems for many years and we have developed an enviable group of knowledgeable people on this subject.

PT: What are the future plans of Motorola in the Field of SCADA Systems?

DB: We understand that work in the security area is never done. We released a new enhanced security package for SCADA late last year and we are now discussing ways to improve that offering.

PT: Whilst thanking you for time, Steve permit me to ask you one last question, on what is your advise to companies who run SCADA system, but haven't thought of security yet

DB: My advice to such companies is to have a security risk assessment performed so they at least will understand their general situation and can plan ahead to address the most serious problems they may encounter.

PT: Thank you for the interview.

PENTEST TEAM

Homeland Security

Reducing the Threat from Attacks

This article is written to describe the changes being made in the Homeland Security activities for new software in development, and how they are improving our overall security. The reader may also find which activities can fit into their Software Development Lifecycle (SDLC) programs to further benefit other organizations as well. This is not an offensive approach to Cyber Security, but an improved defensive approach.

Every day the United States Government is subject to cyber-attacks which threaten the lives of citizens and agency missions. Threat agents include other countries, citizens of the United States, and organized crime (to name a few). The US Department of Homeland Security has the responsibility of protecting Federal systems and supporting other agencies of the US Government with protecting information and reporting cyber incidents.

The actual source of the attacks is usually unpredictable (it would certainly make it easier if they would announce their intentions in advance), though most have similar objectives, to get the information that organizations are trying to protect. Attacks on information systems can be easily spoofed, thereby making the source IP address a non-reliable source of the connection. Open source projects such as the TOR network, bot nets, and other infected resources make investigations more challenging [1]. At present, most Federal agencies approach securing the homeland through defensive measures which are largely reactionary. The lack of proactive measures places these agencies in a losing battle.

Attempting to identify the source of an attack is not trivial, as attacks are generally carried out by systems that have been compromised. Ultimate-

ly, the source of the problem is insecure software. As such, agencies can better protect their systems by building security into their software [2]. Although a wealth of information exists to support building better software (see Microsoft's SDL or Cigital's Software Security Touchpoints), most organizations encounter problems when trying to transition from theory to practice.

Regulation and Compliance to the Rescue?

Congress passed the E-Government Act of 2002 to address the lack of security within Federal information systems. Title III of the E-Government Act, the Federal Information Security Management Act (FISMA), was designed to promote responsibility for security through mandate. FISMA mandates that organizations report their security posture as measured by standards published by the National Institute of Standards and Technology (NIST). The security standards identify a minimum set of security requirements for information and information systems.

The result is the development of a process drawing on security requirements that falls short in terms of defining how organizations can implement these standards, as well as how each organization can measure the effectiveness of their programs.

FISMA is grounded in following processes and demonstrating compliance with checklists. Unfortunately, FISMA fails to offer the organizations the value of improving the overall security of their systems as FISMA focuses the government on processes and reporting which competes for security funding, usually to the detriment of actual security operations.

FISMA identifies the classification of federal systems as Low, Moderate, or High vis a vis FIPS publication 199 [3]. FIPS 199 defines the standards for Security Categorization of Federal Information and Information Systems. Depending on the identified classification of systems, FISMA relies on NIST special publication 800-53 [4] which proscribes an increasingly restrictive set of security controls depending on the classification of federal systems. The intent of this publication is to allow the security practitioner to customize controls which are related to the system and the security classification. Using the NIST 800-53 controls, the organization is able to better classify the security issues, and activities needed to obtain accreditation for use.

Unfortunately, one of the major drawbacks of NIST 800-53 is the failure to bridge information security theory with information security practice.

Is Pentesting Enough?

Pen Testing the environment is often used as the primary means of determining the security of systems. A drawback of using penetration testing as a sole mechanism for securing systems lies in the late stage of SDLC where testing occurs. Because penetration testing occurs once a system is production ready, the earlier stages of the SDLC are often overlooked (for example sometime after code is running, a decision is generally made to run a 'Pen Test'; exactly what is being tested is not necessarily clear.)

Another issue with pen testing relates to the level of systems coverage. At Cigital, we have found that the Pen Test exercise covers only a small fraction of the actual codebase. For this reason, Cigital refers to Pen Tests as being a "Badness-ometer". For example, when a pen test is performed on a system and several findings are discovered, the system is clearly insecure. However, if a pen test is performed and no findings are discovered, does this mean that the system is secure? Most likely the answer is "no". Just because a security practitioner did not discover a vulnerability, the system

may still have vulnerabilities which have not been discovered (remember, the pen test only covers a small percentage of the codebase). For this reason, we can state that pen testing is not enough. The rule of thumb is that a pen test will only tell you how bad your code is, not how good. As a result, the pen test is really a badness-ometer.

A New Approach for Securing Systems?

The traditional approach to cyber security has been reactive. The traditional approach is mired in an improper interpretation of "Defense in Depth". Systems and networks are hardened at the perimeter of the network and include a multitude of tools which operate as filters throughout the cyber infrastructure. We like to call this the M&M defense (hard on the outside, and soft in the center). The underlying assumption is that adding more and more security products and services will inevitably reduce the attack surface and eradicate risk.

One of the problems with "securing the perimeter" lies in the faulty assumption that networks have boundaries which can be defined. With the rise of cloud and mobile computing, the security team is left scratching their heads with respect to where the boundaries are and how to define them. When you boil down the challenge, the least common denominator falls on the assurance of the software and software applications. Simply put, if you can establish an assurance level for deployed software, you will better understand where your weaknesses lie.

This has been a resounding within organizations and the number one reason that Cigital was called upon by DHS to assist in the deployment of Static Analysis tools and the development of the Build Security In initiative.



Badness-ometer

Figure 1. Pentests are only a small measure of "Badness"

Where do you Fix the Bugs?

When considering the total cost of ownership for a software application, the benefits of implementing software security are considerable. Consider the diagram shown on Figure 2.

Figure 2 identifies that the cost of remediating vulnerabilities at later stages of the development life cycle is far greater than the cost of remediating vulner-

abilities at earlier stages of the life cycle. In fact, the diagram shows that while the average cost of fixing a single vulnerability during the early stages of development is \$977, the cost of remediating vulnerability at a later stage is \$14,102 (that's a factor of 14 times higher!). Maybe you're asking, but how can I fix the bugs, if I am testing the software with Pen Tests? Let's approach this matter one step at a time.

Cost of Fixing Critical Defects

Cost of Fixing Vulnerabilities EARLY				Cost of Fixing Vulnerabilities LATER			
Stage	Critical Bugs Identified	Cost of Fixing 1 Bug	Cost of Fixing All Bugs	Stage	Critical Bugs Identified	Cost of Fixing 1 Bug	Cost of Fixing All Bugs
Requirements		\$139		Requirement		\$139	
Design		\$455		Design		\$455	
Coding	200	\$977	\$195,400	Coding		\$977	
Testing		\$7,136		Testing	50	\$7,136	\$356,800
Maintenance		\$14,102		Maintenance	150	\$14,102	\$2,115,300
Total	200		\$195,400	Total	200		\$2,472,100

Identifying the critical bugs earlier in the lifecycle reduced costs by \$2.3M

SOURCE: Digital, "Case Study: Finding Defects Earlier Yields Enormous Savings"

Figure 2. The cost of remediating vulnerabilities

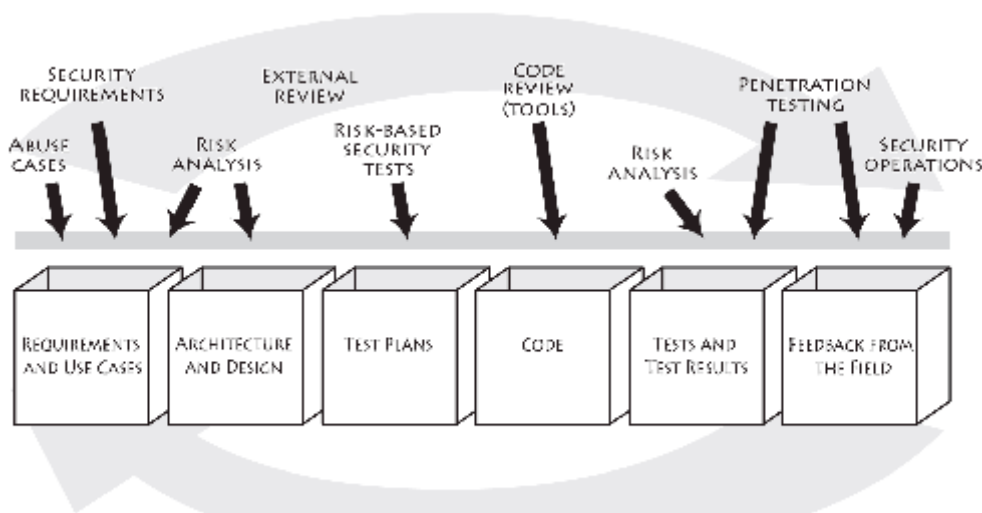


Figure 3. Cigital's Software Development Life Cycle (SDLC) with Security Related activities

Bugs Should Be Fixed in Development

The higher expense is usually incurred by detecting vulnerabilities late in the development process. Consider the Figure 3. This figure presents the SDLC as indicated by the boxes and provides security Touchpoints for how security can be introduced at various stages of the SDLC. As you can see, we have inserted Security activities in each of the SDLC phases (you can read about these exercises and the security touch points in Software Security by Gary McGraw) (While our figure is more representative of a waterfall approach, the iterative SDLC process can adopt it easily) [5].

Many times the overall size of the architecture and complexity of the environment can only be evaluated after the initial development or deployment has already been made. While employing the security controls for an application has been known to be accomplished after the design is completed, continuing to scrutinize the security of an environment after the implementation of the system is completed is a kin to trying to bolt security

on top of the environment (as opposed to creating it inside the application). (McGraw)

This is not to say that we should stop using FIS-MA or halt the use of Pen Testing activities at all, because these activities are essential to determining the correct implementation of security in the enterprise. However, changing or augmenting the traditional testing during the SDLC has been shown to improve the security of the application, as well as help to fix the security posture of the application before it reaches production.

Digital has taken a different approach to Software Security; we recommend the implementation of security directly into the software. This approach enables the developers to be an active part of the active security team. The chart in Figure 3 looks at the development of new software and how security related activities are always a part of the Software Development Life Cycle (SDLC).

As we can see from Figure 3, the actual introduction of Pen Testing is far to the right of the SDLC, very near the production phase. This is very late

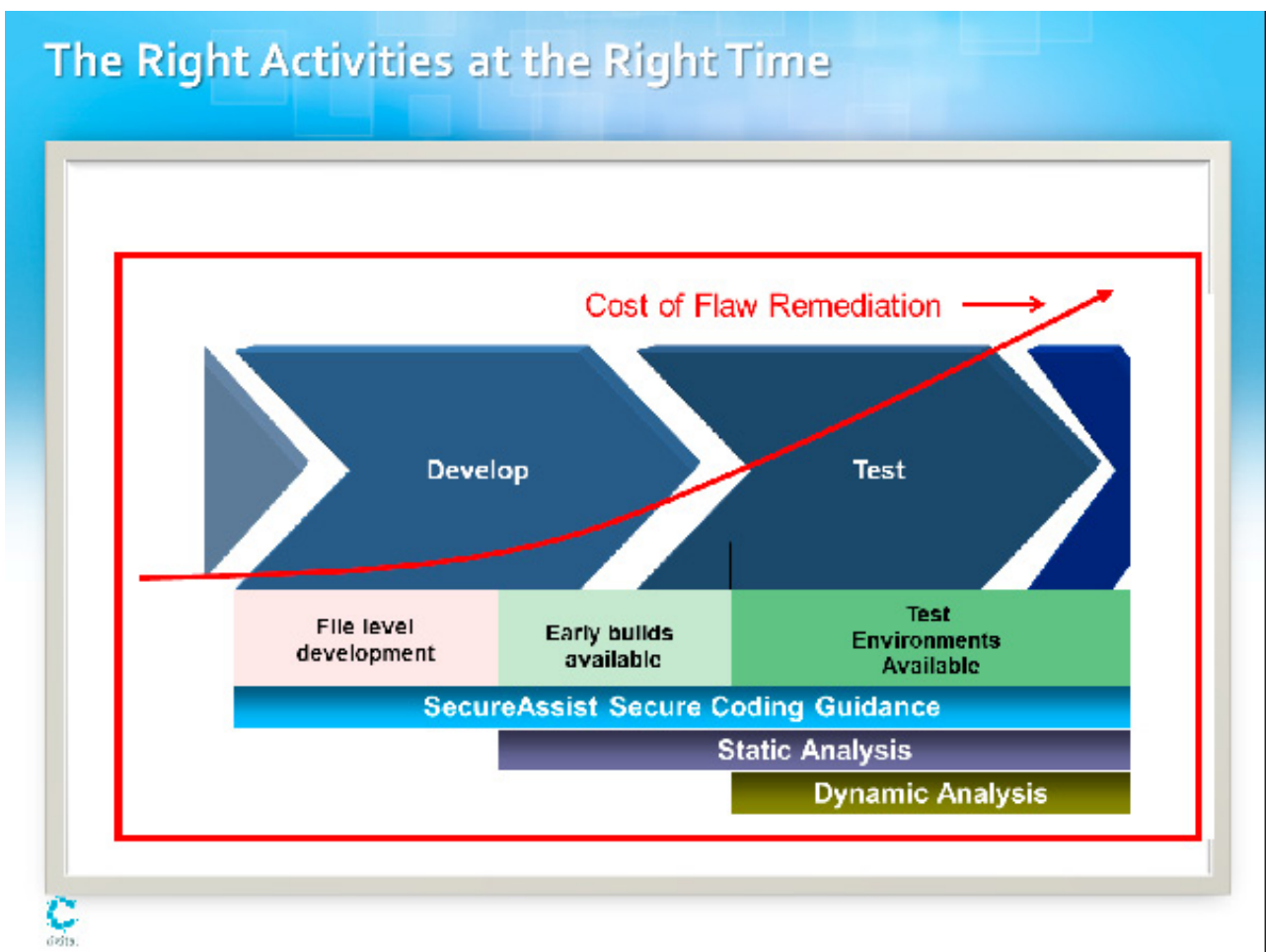


Figure 4. Security activities for new development

in the SDLC process and also complicates the updates for the software to implement better security into the software.

By enabling the developers to implement better security directly into the software while it is on their desktop, we minimize the delays to improve the overall security of the software. This is an essential component to implementing better security controls.

Code Review

Here are some of the code review functions which Digital is providing to its clients, as well as to the Department of Homeland Security (and other government agencies within it as well). This explains why the cost of fixing bugs is so costly in the Testing phase, Figure 2.

Figure 4 outlines three different activities which Homeland Security has undertaken as part of their new understanding of security development. The three activities listed above include:

- SecureAssist Secure Coding Guidance (training the developers)
- Static Analysis
- Dynamic Analysis
- Binary Analysis [6]

We can easily see that the cost of fixing vulnerabilities is significantly lower the further left we are in the development process. This is what we are discussing when we say that we want to enable the developers to become more proactive for fixing security issues. Since the developers already have the software on their desktop, they are the best choice to make the changes, before bugs are introduced into the software.

SecureAssist Secure Coding Guidance is a plugin that is provided to the developers Integrated Development Environment (IDE). SecureAssist changes the security stance from reactive remediation to proactive security. Instead of focusing on new ways to find bugs already in the code base – organizations should provide developers with the guidance they need to build expertise and to PREVENT bugs from entering the code base.

One of the best things about the SecureAssist plugin is that it does not require access to running code or code that compiles completely. It actually supports the developer working on the file(s) that the developer has access to, and works in real-time, compared to other testing activities. This tool

examines one or more files or the complete project as well.

Static Analysis code review is usually performed after the project has succeeded in producing code that compiles completely. Software which compiles with errors can introduce false findings (either positive or negative), and are usually integrated into the Build Cycle of the SDLC. Static Analysis results then need to be examined and distributed back to the development team in order to fix the vulnerabilities.

Static analysis reviews have always seemed to provide more results on the code base than Dynamic Analysis [7]. While Static Analysis requires that the source code be available for a full review, the complexity of the tools require that Security Analysts (or Developers) run the tools, and then follow-up on all of the findings presented.

Dynamic Analysis is the testing of web based applications which are connectable via the network (Usually available via a web server) [8] or are connectable from a SOAP interface. Dynamic Analysis (You can use a Tool, or Manual examination to perform a Pen Test) [9] is a great testing tool to further validate the effectiveness the security updates to the environment throughout the SDLC.

The difference with Dynamic Analysis is that the testing must be performed on a live application. Most testing is performed on applications within the pre-production environment as dynamic analysis will aggressively test the application, making modifications (like a hacker is able to do) which will change the website. This type of testing should also be performed after implementing a full backup of the environment as well.

The first three testing types have well defined activities for evaluating the security of the new application. The last type of testing is Binary Analysis depends on the ability to test the actual binaries used in the application. This type of analysis is performed on software that is normally bought from another resource or is developed outside of the controls that the organization has put into place.

Binary Analysis is useful in examining resources which cannot be reviewed with static or dynamic analysis.

Because Homeland Security activities are dependent on the security of the organization from hackers, the largest areas of activity for attacks are seen coming from network (internet/intranet) connected resources. These systems are hosted by Private Enterprise solutions, insuring that 50% of

the Security issues are related to the Architecture, and 50% are related to the software within.

As we can see, there are detailed activities and controls which have been developed to support the security of the network and architecture overall. That leaves us with 50% of the environment to work on, the software to improve its security.

BSIMM

As I mentioned earlier, the BSIMM model is currently helping organizations to describe the activities that they are currently employing, which begins to outline the holes that remain in order to improve the overall security of the environment (Figure 5).

BSIMM is a descriptive process used to determine the current commitment of the organization for the security program. The example above indicates the overall posture of 51 organizations that are committed to improving the overall security within their organizations. While this outline is a review of the security for private corporations, it can also be easily engaged to determine the posture of different departments within Homeland Security.

Cigital Federal is currently the provider of Software Security Consulting and Training for the Dept. of Homeland Security (DHS) as well as other Government agencies. Using Cigital's 20+ Years of Software Security experience, Cigital Federal is delivering Consulting, Instruction, Products, Analysis and Processes to insure that better Software Security is achieved wherever it is needed.

Whether your needs are securing Homeland Security, a bank, a utility or another organization Cigital has the processes and resources to improve your organizational security.

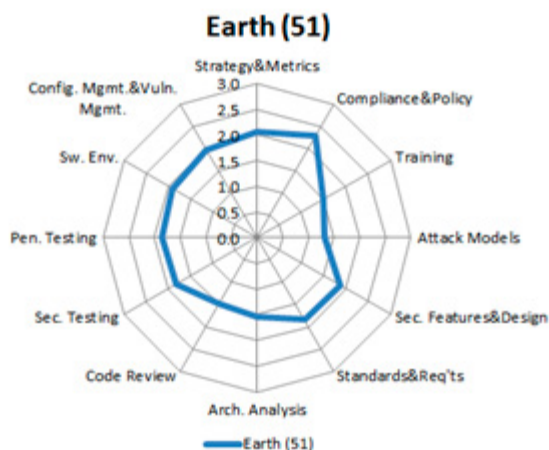


Figure 5. BSIMM review of 51 organizations

References

- [1] Some solutions exist to block entire countries; however this does not stop attacks from compromised hosts within your own country.
- [2] <http://www.cigital.com/products/the-building-security-in-maturity-model-bsimm/>
- [3] <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>
- [4] NIST is currently requesting updates on revision 4 for the 800-53 control set. You can add comment to the security and privacy controls update at <http://www.nist.gov/itl/csd/sp800-020613.cfm>
- [5] While our figure is more representative of a waterfall approach, the iterative SDLC process can adopt it easily.
- [6] While Binary Analysis is not part of the diagram, it can be a useful component of testing.
- [7] Cigital has a unique presence in the Static Analysis environment with the creation of the first Static Analysis tool ITS4. After Cigital sold the license of the ITS4 to an investment group, the tool was later acquired by HP and is now known as HP Fortify.
- [8] Usually available via a web server.
- [9] You can use a Tool, or Manual examination to perform a Pen Test.

Works Cited

- BSIMM. (n.d.). <http://bsimm.com/>
- DHS. (n.d.). <http://www.dhs.gov/>
- FISMA. (n.d.). <http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>. FISMA
- McGraw, G. (n.d.). Software Security – Building Security In. Addison-Wesley Software Security Series
- NIST. (n.d.). NIST 800-53 revision 3 controls. http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated_errata_05-01-2010.pdf

ALBERT WHALE

Albert Whale is a Security Consultant with Cigital Federal in Sterling, VA. Albert resides in Pittsburgh, PA with his wife and three children (three others have escaped already). He has 28 years of Professional experience having worked in Application Development, Systems Engineering, Network Security and Application Security. Albert is the past President and Co-Founder of the Pittsburgh FBI InfraGard, and has been active in the Security field since 9/11. Email: awhale@Cigital.com, LinkedIn: <http://www.linkedin.com/in/aewhale>, Skype: aewhale

How Hackers Get Caught

the True Story

Flaws in Unix-like Rootkits and Anti-rootkit Tools

Most high-profile intrusions of the past decade haven't been found due to intrusion detection sensors or complicated forensic tools. Instead, it was the malfunctioning code in the rootkits that made them crash the system with weird error messages.

Most of you already know that the rootkit is the basic set of tools an intruder uses to keep control over a compromised system. Common features of a rootkit include:

- Remote access,
- Ability to intercept data,
- Hiding modifications on the filesystem,
- Hiding processes,
- Hiding 'magic' users,
- Hiding remote access ports/connections.

There are two types of rootkits, based on the way they interfere with user actions: user land and kernel land rootkits. The difference between them arise from the methods they use to hijack the operating system functions.

Rootkits work by subverting the normal operations of the system, either by modifying files on the system with backdoored versions (*userland rootkits*) or hijack oper-

ating system function/handler pointers in memory to alter normal behavior (*kernel land rootkits*) in order to keep SUPER USER rights.

In order to be able to keep control over a compromised system, a *userland rootkit* has to modify or alter in some way a binary file, either by replacing the file, modifying parts of the file on disk or modifying parts of process memory space. Such modifications are, however, easily spotted by the trained admin eye, because user land rootkis provide poor means to disguise the presence of the attacker and his tools, poor means to hide the remote connection, not many options to survive reboot, etc.

```
# Adore Rootkit. OK, nobody calls it that but basically it uses Adore.
# In one commercial AV vendors naming scheme it's called Dextenea.
AKIT_FILES="${RKHROOTDIR}/usr/secure
${RKHROOTDIR}/usr/doc/sys/qrt
${RKHROOTDIR}/usr/doc/sys/run
${RKHROOTDIR}/usr/doc/sys/crond
${RKHROOTDIR}/usr/sbin/kfd
${RKHROOTDIR}/usr/doc/kern/var
${RKHROOTDIR}/usr/doc/kern/string.o
${RKHROOTDIR}/usr/doc/kern/ava
${RKHROOTDIR}/usr/doc/kern/adore.o
${RKHROOTDIR}/var/log/ssh/old"
AKIT_DIRS="${RKHROOTDIR}/lib/security/.config/ssh
${RKHROOTDIR}/usr/doc/kern
${RKHROOTDIR}/usr/doc/backup
${RKHROOTDIR}/usr/doc/backup/txt
${RKHROOTDIR}/lib/backup
${RKHROOTDIR}/lib/backup/txt
${RKHROOTDIR}/usr/doc/work
${RKHROOTDIR}/usr/doc/sys
${RKHROOTDIR}/var/log/ssh
${RKHROOTDIR}/usr/doc/.spool
${RKHROOTDIR}/usr/lib/kterm"
AKIT_KSYMS=
```

Figure 1. Rootkit detection in RKHUNTER – ADORE

On the other hand, *kernel land rootkits* need to interfere with binaries only during the booting phase, to make sure they are loaded by the system initialization procedure. Also, they provide incredible means of hiding an attacker's presence inside a computer system, by manipulating the most low-level routines of the operating system. Also, they make remote access really easy to the attacker, with little to no warnings to the administrator and they are very hard to detect by rootkit detection tools. However, the complexity of code may result in unexpected behavior.

So how do *anti-rootkit tools* work? They are founded on the principle that the rootkit needs to make certain changes to an operating system in order to work. *User land rootkits* will alter files on disk, timestamps, file sizes, the directory structure, etc. *Kernel land rootkits* alter system calls and functions, most of them focusing on the syscall table. Any type of rootkit will add files to the file system, maybe start new processes or new remote connections. For instance, the fact that rootkits keep the same file structure for their own files, makes them easily spotted by traditional *anti rootkit tools* such *chkrootkit* or *rkhunter*, because these tools use the directory and file structure of rootkits to generate signatures of malware presence (Figure 1-5).

They parse certain system directories looking for files known to be the part of malware, so when such a suspected file is found, the user is alerted.

However, as you can easily see, newer or slightly modified versions of rootkits go undetected by traditional signature scanning methods, therefore there appears the need of a periodically updated database with latest rootkit signatures, and even then there is no guarantees that a rootkit did not evade the signature scan.

The new technology has been developed in order not to have to rely on signatures or known-to-be-sane system fingerprints to scan for. Instead, it uses live system information it gathers to be able to heuristically determine signs of rootkit activity. Furthermore, we are able to uniquely pinpoint the rootkit code, thus being able to analyze it and determine its exact functionalities, and also extract a unique signature specific to the typology of the

```
# Adore Rootkit. OK, nobody calls it that but basically it uses Adore.
# In one commercial AV vendors naming scheme it's called Dextenea.
AKIT_FILES="${RKHROOTDIR}/usr/secure
            ${RKHROOTDIR}/usr/doc/sys/qrt
            ${RKHROOTDIR}/usr/doc/sys/run
            ${RKHROOTDIR}/usr/doc/sys/crond
            ${RKHROOTDIR}/usr/sbin/kfd
            ${RKHROOTDIR}/usr/doc/kern/var
            ${RKHROOTDIR}/usr/doc/kern/string.o
            ${RKHROOTDIR}/usr/doc/kern/ava
            ${RKHROOTDIR}/usr/doc/kern/adore.o
            ${RKHROOTDIR}/var/log/ssh/old"
AKIT_DIRS="${RKHROOTDIR}/lib/security/.config/ssh
            ${RKHROOTDIR}/usr/doc/kern
            ${RKHROOTDIR}/usr/doc/backup
            ${RKHROOTDIR}/usr/doc/backup/txt
            ${RKHROOTDIR}/lib/backup
            ${RKHROOTDIR}/lib/backup/txt
            ${RKHROOTDIR}/usr/doc/work
            ${RKHROOTDIR}/usr/doc/sys
            ${RKHROOTDIR}/var/log/ssh
            ${RKHROOTDIR}/usr/doc/.spool
            ${RKHROOTDIR}/usr/lib/kterm"
AKIT_KSYMS=
```

Figure 2. Rootkit detection in *RKHUNTER – SUCKIT*

```
# Phalanx Rootkit
PHALANX_FILES="${RKHROOTDIR}/uNFuNF
               ${RKHROOTDIR}/etc/host.ph1
               ${RKHROOTDIR}/bin/host.ph1
               ${RKHROOTDIR}/usr/share/.home.ph1/phalanx
               ${RKHROOTDIR}/usr/share/.home.ph1/cb
               ${RKHROOTDIR}/usr/share/.home.ph1/kebab"
PHALANX_DIRS="${RKHROOTDIR}/usr/share/.home.ph1
              ${RKHROOTDIR}/usr/share/.home.ph1/tty"
PHALANX_KSYMS=

# Phalanx2 Rootkit
PHALANX2_FILES="${RKHROOTDIR}/etc/khubd.p2/.p2rc
                ${RKHROOTDIR}/etc/khubd.p2/.phalanx2
                ${RKHROOTDIR}/etc/khubd.p2/.sniff
                ${RKHROOTDIR}/etc/khubd.p2/sshgrab.py
                ${RKHROOTDIR}/etc/lolzz.p2/.p2rc
                ${RKHROOTDIR}/etc/lolzz.p2/.phalanx2
                ${RKHROOTDIR}/etc/lolzz.p2/.sniff
                ${RKHROOTDIR}/etc/lolzz.p2/sshgrab.py
                ${RKHROOTDIR}/etc/cron.d/zupzzplaceholder
                ${RKHROOTDIR}/usr/lib/zupzz.p2/.p-2.3d
                ${RKHROOTDIR}/usr/lib/zupzz.p2/.p2rc"
PHALANX2_DIRS="${RKHROOTDIR}/etc/khubd.p2
               ${RKHROOTDIR}/etc/lolzz.p2
               ${RKHROOTDIR}/usr/lib/zupzz.p2"
PHALANX2_KSYMS=
```

Figure 3. Rootkit detection in *RKHUNTER – PHALANX*

rootkit that can be used to speed up further scans, and also, to heuristically determine new or slightly modified versions of the rootkit.

So, how do newer rootkits get detected using traditional means? Well, they don't. Instead, rootkits make visible changes to the operating system, sometimes resulting in system crashes and weird error messages, mostly due to insufficiently tested code. For example, Phalanx tries to disguise itself as Xnest to access /dev/mem without checking if there is Xnest on the system. An admin would be irritated seeing a message such as "Program Xnest tried to access /dev/mem between 0->8000000" when he doesn't even have Xnest running. And other kernel rootkits have their own distinctive flaws.

So, basically, rootkits are found because they hijack predictable places, mostly aiming at the syscall table, Interrupt Descriptor Table or hijacking filesystem operations. Most modern anti-rootkit detection tools check all these places for inconsistencies with the values previously gathered in their database making visible such a modification. The major flaw of this approach is that if the system is already compromised, or if the attacker has access to the stored fingerprint, or fingerprint update mechanism, they can easily get unnoticed.

Another problem of a rootkit is that usually they tend to employ as many functionalities as possible, and complex code is a very dangerous bet, especially in Kernel land as it increases the number of possible points of failure. Also, most rootkits don't get a consistent grasp of the specifics of the system they run on.

Another major problem of a rootkit is the *remote access*, because an alert admin could easily spot unknown traffic going to suspicious ports, especially if it's encrypted or encapsulated. Eavesdropping the connection can provide important informations about the intruder.

But as we can easily realize, current Unix anti-rootkit tools provide little to no accuracy in detection of rootkits, the impossibility to clean the system from a rootkit infection or the ability to analyze the malware. It looks like anti-rootkit tools have to step the notch a bit and raise the bar a little higher for rootkit programmers, so that they come up with better and newer detection mechanisms, not relying on known fingerprints or signatures, as these can easily be evaded or forged.

```
if [ "${EXPERT}" = "t" ]; then
[ -r /proc/ksysms ] && $(egrep) -i "adore|sebek" < /proc/ksysms 2>/dev/null
[ -d /proc/knack ] && $(ls) -la /proc/knack 2>/dev/null
PV=$(ps -V 2>/dev/null) | grep -d " " -f 3 | $(awk) -F . '{ print $1 "." $2 $3 }' | $(awk) '{ if ($0 > 3.19) print 3; else if ($0 < 2.015) print 1; else print 2 }'
[ "${PV}" = "" ] && PV=2
[ "${SYSTEM}" = "SunOS" ] && PV=0
expertmode_output "./chkproc -v -v -p $PV"
return 5
fi

### adore LPM
[ -r /proc/ksysms ] && \
if $(egrep) -i adore < /proc/ksysms >/dev/null 2>&1; then
echo "Warning: Adore LPM installed"
fi

### sebek LPM (Adore based)
[ -r /proc/ksysms ] && \
if $(egrep) -i sebek < /proc/ksysms >/dev/null 2>&1; then
echo "Warning: Sebek LPM installed"
fi
```

Figure 4. Rootkit detection in CHKROOTKIT – ADORE

```
## Suckit rootkit
expertmode_output "${strings} ${ROOTDIR}/sbin/init | $(egrep) HOME"
expertmode_output "cat ${ROOTDIR}/proc/1/maps | $(egrep) init."
expertmode_output "cat ${ROOTDIR}/dev/.golf"

### Suckit
if [ -f ${ROOTDIR}/sbin/init ]; then
if [ "${QUIET}" != "t" ]; then printn "Searching for Suckit rootkit... "; fi
if [ "${SYSTEM}" != "HP-UX" ] && ( $(strings) ${ROOTDIR}/sbin/init | $(egrep) HOME || \
cat ${ROOTDIR}/proc/1/maps | $(egrep) "init." ) >/dev/null 2>&1
then
echo "Warning: ${ROOTDIR}/sbin/init INFECTED"
else
if [ -d ${ROOTDIR}/dev/.golf ]; then
echo "Warning: Suspect directory ${ROOTDIR}/dev/.golf"
else
if [ "${QUIET}" != "t" ]; then echo "nothing found"; fi
fi
fi
```

Figure 5. Rootkit detection in CHKROOTKIT – SUCKIT

AB CONSULTANCY SOFTWARE SRL

Is a newly merged computer security company located in Bucharest, Romania whose main area of activity is penetration testing and forensics examination. Our experts have over 20 years of international experience in the field of computer security research, both offensive and defensive security, ranging from malware and antimalware research, software audit, exploit development or cryptology. Our customers are government, military or financial industries, both based in Romania or abroad.

Begin Your Journey to a Secure Software Supply Chain

Learn Best Practices from the latest Feature Supplement of Veracode's State of Software Security Report

Study of Enterprise Testing of the Software Supply Chain

Veracode's study found that enterprises with a programmatic approach had **approximately 10 times more** vendors and applications participating in their programs than enterprises with an ad-hoc approach.

	Vendor-Supplied Software Testing Approaches	
	Enterprises with an Ad-Hoc Approach	Enterprises with a Programmatic Approach
Average number of vendors participating	4	38
Average number of applications assessed	7	71
Percent of applications achieving compliance	34%	52%
Percent of applications achieving compliance within one week	28%	45%
Percent of non-compliant applications that are out of compliance for more than six months	39%	20%

approximately
**10 TIMES
MORE**

**LOWER
IS BETTER**

This featured supplement focuses on the state of enterprise programs that assess the security of software purchased from vendors. Veracode can uniquely report on how program practices evolve because our analysis is based on data aggregated from companies as they test real applications.

VERACODE



Download the full report:

<http://www.veracode.com/reports/index.html>

Or scan to download the latest supplement of Veracode's State of Software Security Report

Veracode is the only independent provider of cloud-based application intelligence and security verification services. The Veracode platform provides the fastest, most comprehensive solution to improve the security of internally developed, purchased or outsourced software applications and third-party components. Learn more at www.veracode.com

Security Concern in

FemtoCell-Our own Base Station

“Coverage” is a key term for all telecom operators. Providing coverage is always a challenge for them. Day by day mobile users are increasing and because of this growth mobile operators are very constraint for bandwidth. That’s why we are facing coverage problem and sometimes unable to connect to mobile users in an emergency. The concept behind this problem is known as cell splitting.

In a general telecom network, the number of serving base station is equal to number of cells. When mobile users increase, then network traffic increases, and hence number of base station will increase. A cell is directly depended on the base station, so telecom operators have to increase cell size. This principle is known as Cell Splitting.

Cell Splitting Principle in Femtocell

Telecom operators use cell splitting to reduce network traffic and provide better coverage and voice quality to users by implementing a concept of “femtocell”. Femtocell is a small Access point or you can say your own Base station with coverage less than 50m. It is developed for enhancing 3G connectivity meaning higher bandwidth and better voice quality. A Femtocell operates in licensed spectrum and provides connectivity to mobile devices for connecting to the mobile network via a broadband connection. For accessing a femtocell the mobile number should be registered. Once it is registered the mobile receives an SMS with a hidden OTA with the reconfiguration commands. The SIM Card gets reconfigured according to the commands and thus enabling the mobile device to connect to the femtocell.

In short, we can list the advantages of femtocell for users as well as for operators.

Advantages of Femtocell

Using femtocell has lots of advantages for users as well as for operators.

Advantages for Users

- Installed at home so high voice quality, distortion free signal and more coverage.
- Low Power Usage
- High dedicated bandwidth
- Location Service (Need to search)
- Provide Landline support

Advantages for Mobile Operators

- No Installation and maintenance cost
- Less manpower required as no need of going and installing at user side.
- Traffic reduction, giving a high quality signal hence overall quality service increased
- Cheap hardware
- No investment on extra base stations, or their maintenance etc.
- Customer satisfaction at low cost

Femtocell Architecture

The Figure 1 shows mobile users directly connected to the Femtocell Access Point (FAP). The num-



ber of users that can connect to FAP depends on the FAP capacity. A FAP is connected to the SeGW using the public IP network and after mutual authentication it may allow connection to the Femto-cell Management System (FMS)

There are two possibilities for the FMS:

- Inside Operators Core Network
- Outside Operators Core Network (Public Internet)

When the FMS is inside the operator's core network, then a FAP has to communicate to the FMS through the *Security Gateway (SeGW)*. So before connecting to the FMS a subscriber has to verify his identity to the SeGW and vice versa. Every organization protects its infrastructure by implementing a high level of security. Attacking an FMS inside the operator's core network is more difficult as compared to if it was located outside the operator's network (available on public Internet). Since the communication between the FAP and SeGW is on the IP network, it is assumed to be untrusted and that's why before connecting the FAP to FMS it is essential to authenticate the FAP. Inside the operator's core network there is an entity AAA (Authentication, Authorization and accounting server) which is used to authenticate the FAP on the basis of stored authorization related credential information.

The main purpose of the AAA server is to control who is allowed (Authentication), what to allowed (Authorization) and tracks the user's activity (Accounting), so a proper security policy should be adopted by an organization. Lacking the security protocol and policy for protecting the resources can be a serious issue.

Sometimes a FAP fails to connect to the SeGW, in this case the operator's uses an outside FMS to connect via the public internet to diagnose the problem. If the FMS is outside of the operator's core network it will not be as secure as if the FMS was inside the network.

An attacker can take this advantage to try to break the communication between FAP and FMS and for this reason mutual authentication with secure communication is essential. Authentication is achieved by use of mutual certificates for authentication while secure communication is accomplished using a TLS connection.

[GEEKED AT BIRTH]



You can talk the talk.
Can you walk the walk?

[IT'S IN YOUR DNA]

LEARN:

- Advancing Computer Science
- Artificial Life Programming
- Digital Media
- Digital Video
- Enterprise Software Development
- Game Art and Animation
- Game Design
- Game Programming
- Human-Computer Interaction
- Network Engineering
- Network Security
- Open Source Technologies
- Robotics and Embedded Systems
- Serious Game and Simulation
- Strategic Technology Development
- Technology Forensics
- Technology Product Design
- Technology Studies
- Virtual Modeling and Design
- Web and Social Media Technologies

www.uat.edu > 877.UAT.GEEK

There are two ways used in femtocells to authenticate a subscriber and operator.

Certificate Based Authentication

X.509 certificates are used for authentication over IP Based networks. The FAP and SeGW authenticate each other by the mutual sharing of trusted X.509 certificate using IKEv2. IKEv2 is considered secured because:

- It uses symmetric key share between both FAP and FGW.
- Public key is embedded in the certificate and private key is only known to one of the entities.
- Password known to both FAP and FGW.

The certificate is issued by the manufacturer during the manufacturing process and signed by a Certification Authority. The private key of this certificate is stored securely inside the FAP. This FAP Certificate contains the serial number of the FAP. This is a global key which is fixed during the lifetime of a FAP. (FEID Example) This key is directly given by an operator to the manufacturer and it is hardcoded in the FAP. This key is used with a subscriber's public key. After the mutual authentication is performed successfully, a trusted link between the FAP and SeGW is established using IPSec tunnel. IPSec protocol works in 2 modes:

Transport

In this mode only data to be transferred encrypted while the IP Header is not. If Authentication Header is used, then transport as well as application layer are secured because of hashing.

Tunnel

Both header and data is encrypted and then encapsulated into a new IP packet with a new IP header.

SIM Card Based Authentication

This is a traditional method for authenticating handsets. Authenticated information is stored inside the SIM Card and it has to be installed inside the FAP. So while connecting to the SeGW, the AAA server communicates with the HLR and the Authentication Center (AuC) for authenticating the subscriber according to the stored information inside HLR and AuC.

FAP Security Concerns

Authentication

It is achieved by mutual certification exchange. This certificate is issued by the manufacturer during manufacturing and signed by a Certification Authority. The FAP stores sensitive information like the private key of the certificate securely which is not exposed outside. The key used to sign the cer-

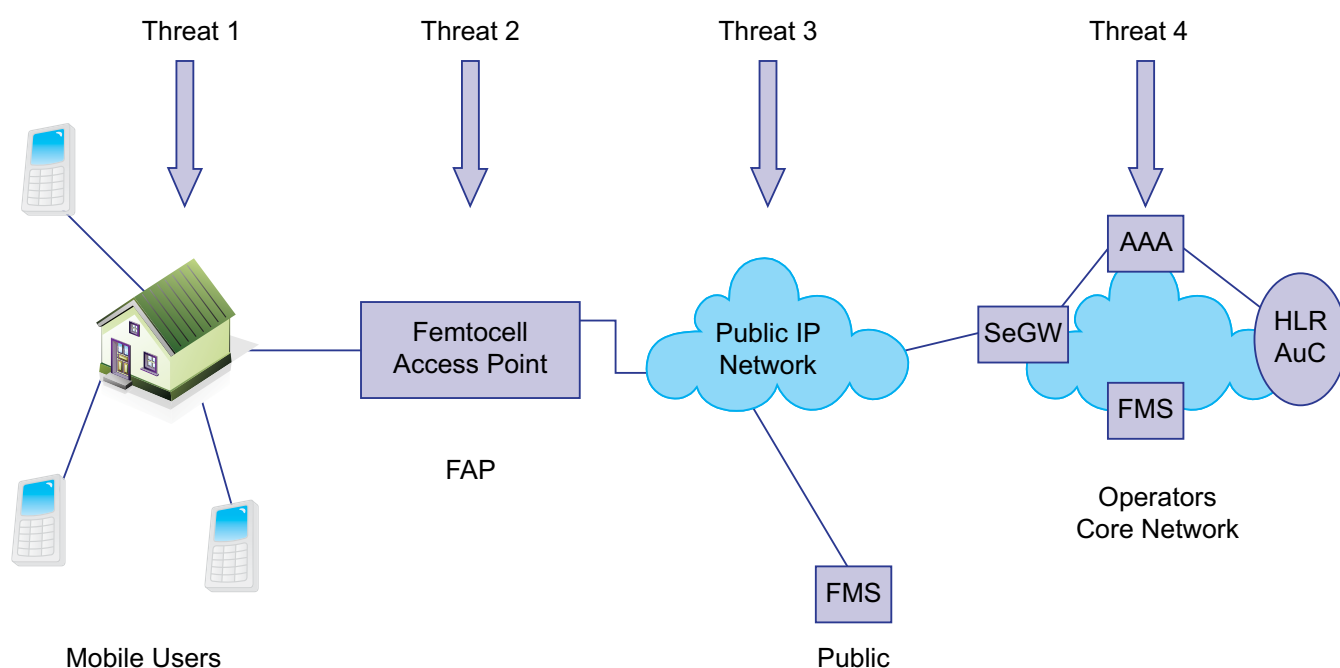


Figure 1. Threat points in Femtocell architecture

tificate is at least 2048 bits and algorithm SHA256 with RSA encryption.

Authorization

It is achieved by FEID(FAP equipment identifier).

Integrity Protection

HMAC and AES-XCBC-MAC-96 is recommended.

Confidentiality Protection

This is achieved by using AES with a minimum 128 bit key in CBC mode.

Device Integrity

This can be achieved during boot up process. Before connecting to the SeGW it performs device integrity checks by matching trusted values with cryptographic hash values and if matches then the FAP boot up process is successful.

Need of Security in femtocell

Few of the most concerning points of femtocell security

- Femtocells are located at user side, so it need to be more secur
- It's out of the operators control and monitoring. ilf user is not aware of security practices then it would be very easy for an attacker to exploit the femtocell Access Point.
- Communication travels over the Internet so it must be kept private and secure.
- Using an IP link so chances of attacks are greater.
- Connecting in the link between FAP and operator's core network and sending unauthorized messages can create a Denial of Service attack.
- Closed Subscriber mode of a femtocell allows connection to the femtocell those who are subscribed (are in the access control list).While in Open Access Mode anyone can connect to femtocell. So it is important to configure femto-cell modes.

Attackers Eyes

Few of the important cases where one need to be careful.

- Check Proper Update in FAP: Organizations using the software update feature to provide their customers better service, improve per-

formance and security enhancements etc. According to them software update means "Patches" Software/firmware needs to be update periodically as day by day new technologies come and older versions of software become vulnerable so it is very essential to them patched. vulnerabilities by using software update. Software updates in the femtocell is performed by the FAP Server which is located inside the operator's network or may be outside, depend on the operator's policy.

- Communication between the FAP and its server must be secure using TLS or IPSec.
- Location verification is used to ensure that operators have licensed spectrum in that area where FAP is working
- FAP Firewall is implemented or not.
- Proper handover is there between 2 femtocell.
- Femtocells are located at the user side and it will access operator's core network using an IP Link so it will be a *major concern* from a security point. As one can attack the femtocell obtain user credentials and then can access the operator's core network

Possible Attack Scenarios

Few of the possible Attack Scenarios are:

FAP Root Access

If an attacker gets root access to the FAP, then he may change internal configuration and other settings, maybe disable the firewall. Thus anyone who is using this FAP will be a victim. Root Access can be doneseveral ways like scanning open ports and if any are found the attacker could telnet or ssh to the open port(s) then launch attacks on these ports.

Software Update

It is also possible for an attacker to connect the FAP to an unauthenticated server and then it can install any software, spoofing devices etc to perform his desired action.

If the software updating center is compromised (not secured or through internal employees) the attacker can install malicious software.

Memory Attack

Checking flash memory of a femtocell whether to if it contains any secret information like list of registered users. It is also possible that list contains registered mobile number's IMSI, which is unique

identity of sim card. After getting the list, it is possible for an attacker to delete or add users without registering. Adding an international number may charge roaming and deduct money from the victims account

Eavesdropping

As femtocells are used inside the home, most of the time (depends on user) only the owner's phone numbers communicate through that femtocell, but the condition is that all numbers have to be registered in the operator's website. Whenever a femtocell boots, the operator's network provide the femtocell a complete list of registered users. This list is stored inside the device in xml form which can be altered by the attacker allowing the attacker to eavesdrop on their call if he has modified the list and also available within the range of femtocell.

Denial of Service: Attacker can launch DoS attack against a femtocell as well as DDoS against the operator's core network by using multiple femtocells. He may also use software simulation installed on computer and then can launch further attacks.

Booting Femtocell

If the booting process is not secured cryptographically then it is possible for an attacker to modify the boot software. Modification/Change to the software may help an attacker to perform various attacks, for example Man in the Middle Attack.

Thus, a proper security policy should be implemented by operator. This includes strong cryptographic algorithm, User Secret Identity Information should not be reveal and will store only on operators network not on the users FAP, and authentication is based on certificates

Recommendation

- Algorithm with higher strength used for authentication and confidentiality.
- Private Key should be securely stored In the FAP, in a way that unauthorized modification is not allowed.
- FEID should not be reveal.
- Before using a femtocell, proper knowledge of security should be given to customer.
- FAP firewall should be used.
- Booting process should be secured

- Sensitive information like authentication details should not be stored in plain text in the FAP, if stored.
- Use of IPSec and Authentication Protocol like Extensible Authentication Protocol (EAP).EAP is known universal authentication framework for wireless networks.
- Software updates and configuration changes should be signed.
- Femtocell should use special technology to detect physical replacement of components.

Conclusion

As is evident, Mobile usage continues to increase many fold, day after day at an unprecedented pace due to the mass adoption of smart phones, tablets and wireless modems for laptops. This is driving the need for continued innovations in wireless data technologies to provide more capacity, high speed connections and generate large amounts of data traffic to the network along with higher quality of service.

Femtocells are an upcoming need for home users or small business but adding more security measures can make it more reliable and make it worth it to use. Proper security update, strong authentication algorithm and user awareness etc can make it more secure.

Femtocells provide an easy and cost efficient way for mobile operators to offer a more fulfilling user experience and deliver broadband data services indoors – consistently and reliably. Femtocells and Wi-Fi will coexist in the future. Customers and operators both can benefit from femtocell technology if it is used securely

But for this the device must be used intelligently enough to select the most appropriate and secure connection while following security mechanisms.

NITIN GOPLANI

Nitin has been working with Aujas as a Security Researcher in the Telecom Security domain. With a rich back-ground in application, Mobile and network security, Nitin is now involved in researching about new and emerging threats to the Telecom Core Nodes. Apart from Research, Nitin is also involved in assisting in the implementation of security measures for Fixed/ Mobile Network (2g/3G/LTE) and core fixed network systems to regulate access to specific network elements for the secure operation of the core fixed network and all its variants



FORENSICS EUROPE EXPO

24 - 25 April 2013

Olympia, London

ForensicsEuropeExpo.com



The Premier International Forensics Event for Police, Military, Intelligence Agencies, Lawyers, Corporate Forensic Analysts, Laboratories, Government Bodies and Agencies together with leading suppliers, services, equipment and practitioners from across the world.

Conferences – Workshops – Training – Networking – Exhibition

REGISTER FOR FREE ENTRY TODAY

www.ForensicsEuropeExpo.com/digital

Co-located with



COUNTER TERROR EXPO

Sponsored by



In Collaboration with



The Forensic Science Society

Organised in Partnership with



ARE YOU SECURE ?

NULLCON

5TH INTERNATIONAL INFORMATION SECURITY CONFERENCE

ARM exploitation	HTML5 attacks	Web security	Pentesting Smartgrid
Bug bounty programs	Malware design	BYOD security	Mobile code security
Hardware backdooring	Underground market	GSM exploitation	USB modem exploitation



Sponsors and Exhibitors

Microsoft®



Training: 27-28th Feb 2013 | Conference: 1-2nd Mar 2013 | Bogmallo Beach Resort, Goa

FOR BOOKING AND SPONSORSHIP - SPONSOR@NULLCON.NET
OR CONTACT ANTRIKSH SHAH +91-9922900657



Nullcon Conference & Trainings
visit www.nullcon.net

CONTRAST

ASPECT SECURITY

Application Security for JavaEE that *just works!*



Start finding and fixing vulnerabilities
for **free NOW!**

www.contrastsecurity.com

ASPECT SECURITY
Application Security Experts