

Secure Interworking Between Networks in 5G Service Based Architecture

Silke Holtmanns

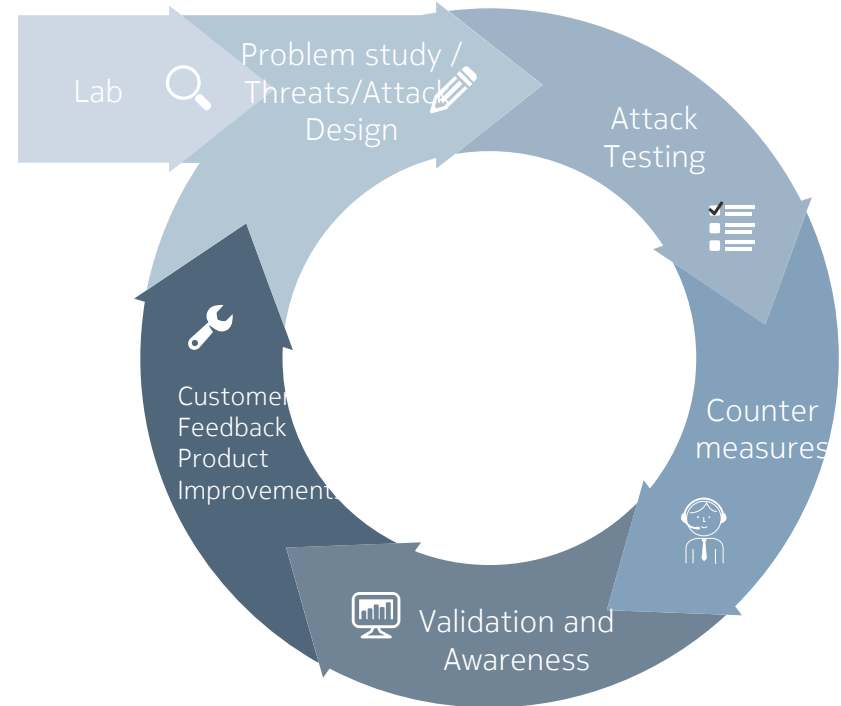
Nokia Bell Labs

Nokia Bell Labs – Future Attacks and Mitigation

Research that solves real problems together with our customers and sometimes even competitors

- Theoretical studies go into attack and countermeasure design
- Validation and awareness of our research by GSMA standards input and publication
- Customer feedback and test results allow us to fine-tune and optimize our countermeasures
- Research input will fit product needs and operators requests
- Operator needs can be discovered "live" for new research challenges and disruptive new solutions

Bell Labs Research Lifecycle



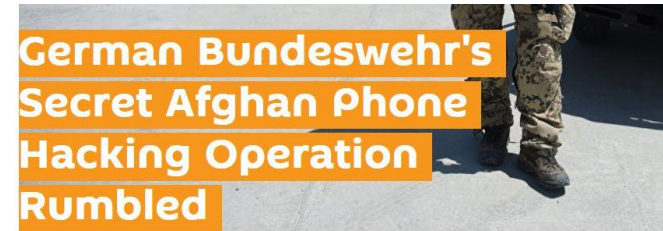
Attacks are reality

Why should attackers stop? Because we have LTE or 5G??

- **Intelligence communities** use mobile networks as a way for VIP tracking and eavesdropping
- **Dark Service companies** use Interconnection to make money (fraud, SMS interception, location tracking offerings)
- **Military** uses mobile network data for target localization

The Switch

New documents show how the NSA infers relationships based on mobile location data



MIDDLE EAST 21:21 24.09.2016 (updated 22:22 24.09.2016) [Get short URL](#) 1 476 0 0

Intercept Implications of 4G/5G Diameter Signaling Replacing SS7

Presented by: *Dr. Jerry Lucas, President, TeleStrategies and a Distinguished Telecom Technology Expert to be announced*

As telecom service providers transition to IP based VoLTE and introduce 5G, SS7 will be replaced with diameter signaling. This session provides the technical basics of diameter, options for transitioning SS7 to diameter and the new challenges facing law enforcement.

Bell Labs

Don't believe it?

- Shodan (or any other IoT search engine will do, search for diameter, sigtran ports or mobile core network nodes that should not be on the Internet).
- Buy access from a service company (Hacking Team)
- Buy access from an unsuspecting operator (search google with wholesale interconnection access, large choice, operators in EU are under pressure)
- Find the targets / spoofing addresses (IR.21 documents on the Internet)



TAPPED



You Can Spy Like the NSA for a Few Thousand Bucks



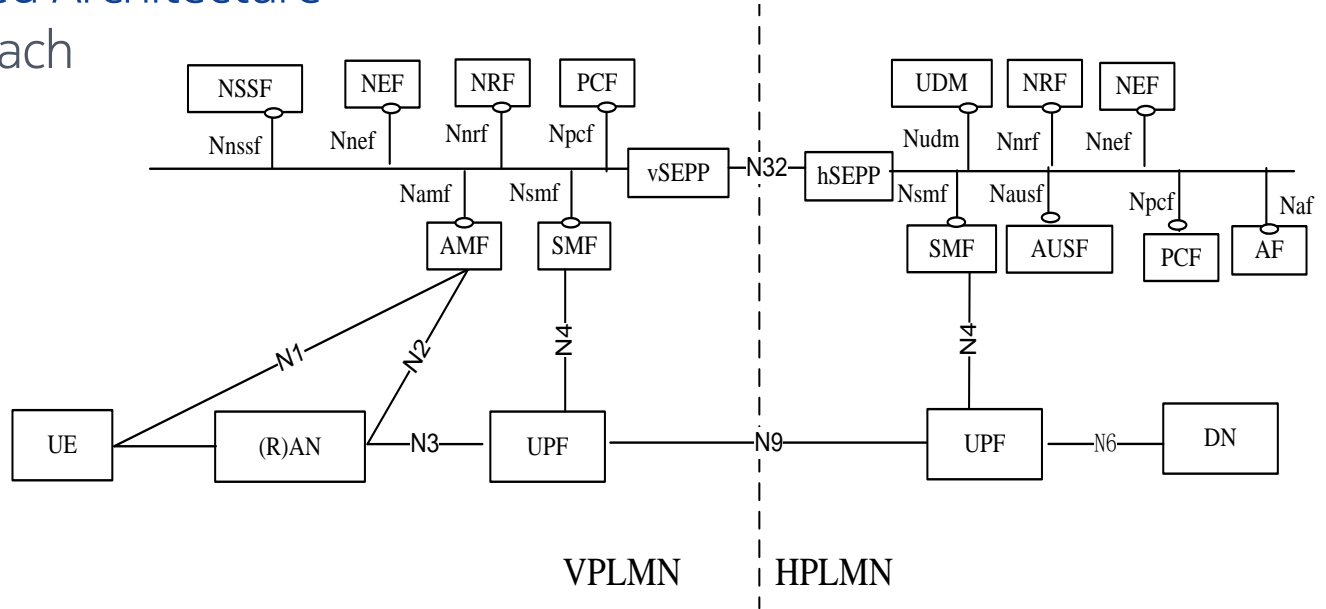
It turns out the highly unsecured SS7 global communications backbone—and a surveillance favorite for spies—is disturbingly cheap and easy to for anyone to get access to.



JOSEPH COX 11.03.17 5:26 AM ET

What about 5G?

Service Based Architecture Bus - Approach



NSSF Network Slice Selection Function
 NEF Network Exposure Function
 NRF NF Repository Function
 PCF Policy Control Function
 SEPP Security Edge Protection Proxy

AMF Access and Mobility Management Function
 SMF Session Management Function
 UE User Equipment
 RAN Radio Access Network
 UPF User Plane Function

AUSF Authentication Server Function
 AF Application Function
 UDM Unified Data Management
 DN Data Network

Rest API – Vulnerabilities are “known” Welcome to the Internet

Remote code execution

Data stealing, authorization fail

DoS

DoS Network? Privilege escalation

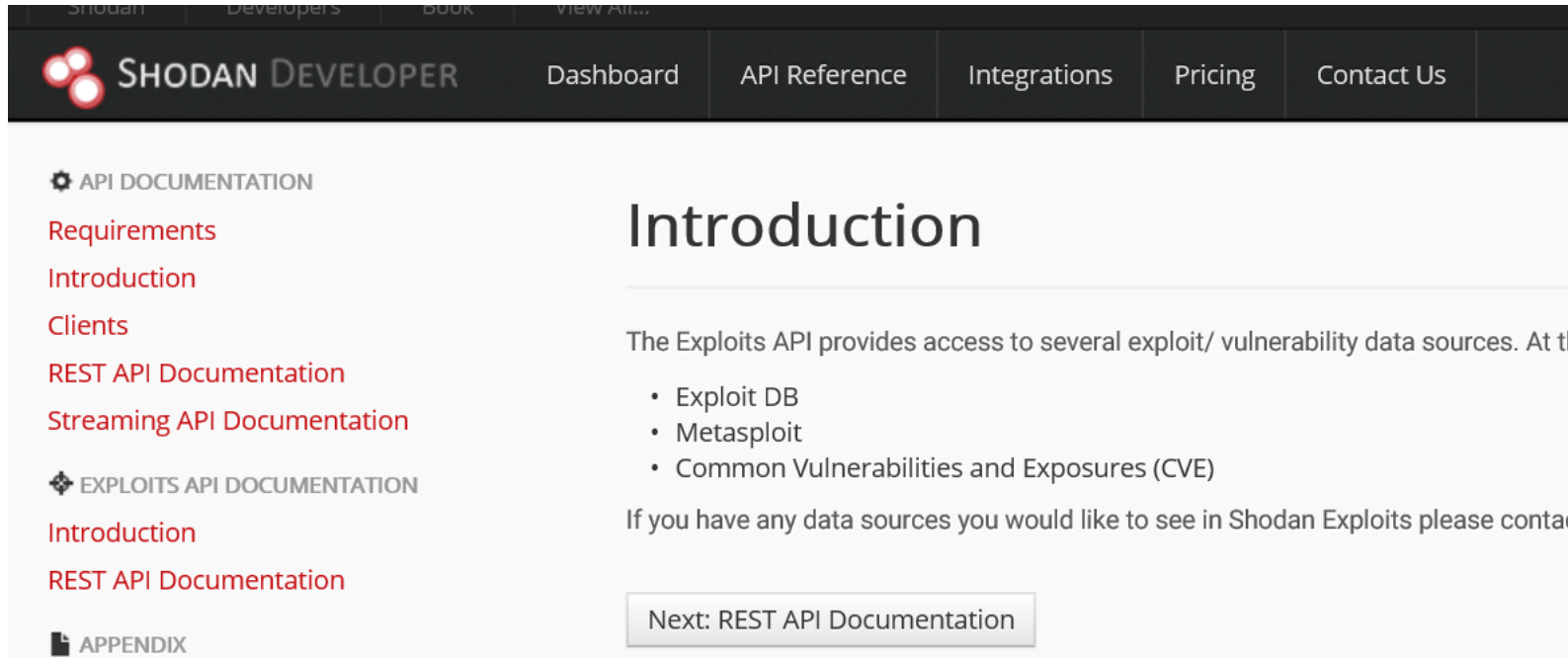
Fraud, data theft

There are 164 CVE entries that match your search.

Name	Description
CVE-2018-9843	The REST API in CyberArk Password Vault Web Access before 9.9.5 and 10.x before 10.1 allows remote attackers to execute arbitrary code via a serialized .NET object in an Authorization HTTP header.
CVE-2018-8849	Medtronic N'Vision Clinician Programmer 8840 N'Vision Clinician Programmer, all versions, and 8870 N'Vision removable Application Card, all versions does not encrypt PII and P...
CVE-2018-7272	The REST APIs in ForgeRock AM before 5.5.0 include SSO tokens IDs as part of the URL, which allows attackers to obtain sensitive information by finding an ID value in a log file.
CVE-2018-5955	An issue was discovered in GitStack through 2.3.10. User controlled input is not sufficiently filtered, allowing an unauthenticated attacker to add a user to the system via the user...
CVE-2018-5261	An issue was discovered in Flexense DiskBoss 8.8.16 and earlier. Due to the usage of plaintext information from the handshake as input for the encryption key used for the...
CVE-2018-1327	The Apache Struts REST Plugin is using XStream library which is vulnerable and allow perform a DoS attack when using a malicious request with specially crafted XML payload. Unlike to the Apache Struts version 2.5...
CVE-2018-1291	Apache Fineract 1.0.0, 0.6.0-incubating, 0.5.0-incubating, 0.4.0-incubating exposes different REST end points to query domain specific entities with a Query Parameter 'orderBy' which are appended directly with SQL statements. A hacker/user can inject/draft the 'orderBy' query parameter by way of the "order" param in such a way to read/update the data for which he doesn't have authorization.
CVE-2018-1289	In Apache Fineract versions 1.0.0, 0.6.0-incubating, 0.5.0-incubating, 0.4.0-incubating, the system exposes different REST end points to query domain specific entities with a Query Parameter 'orderBy' and 'sortOrder' which are appended directly with SQL statements. A hacker/user can inject/draft the 'orderBy' and 'sortOrder' query parameter in such a way to read/update the data for which he doesn't have authorization.
CVE-2018-1274	Spring Data Commons, versions 1.1.3 to 1.1.3.10, 2.0 to 2.0.5, and older unsupported versions, contain a property path parser vulnerability caused by unlimited resource allocation. An unauthenticated remote malicious user (or attacker) can issue requests against Spring Data REST endpoints and endpoints using property path parsing which can cause a denial of service (CPU and memory consumption).
CVE-2018-1273	Spring Data Commons, versions prior to 1.1.3 to 1.1.3.10, 2.0 to 2.0.5, and older unsupported versions, contain a property binder vulnerability caused by improper neutralization of special elements. An unauthenticated remote malicious user (or attacker) can supply specially crafted request parameters against Spring Data REST backed HTTP resources or using Spring Data's projection-based request payload binding that can lead to a remote code execution attack.
CVE-2018-1086	pcs before version 0.9.164 and 0.10 is vulnerable to a debug parameter information disclosure. A remote attacker with a valid token could use this flaw to el...
CVE-2018-1079	pcs before version 0.9.164 and 0.10 is vulnerable to a privilege escalation. The REST interface of the pcsd service did not properly sanitize the file name from the /remote/put_file query. If...
CVE-2018-10732	The REST API in Dataiku DSS before 4.2.3 allows remote attackers to obtain sensitive information (i.e., determine if a username is valid) because of profile pivot's visibility.
CVE-2018-0245	A vulnerability in the REST API of Cisco 5500 and 8500 Series Wireless LAN Controller (WLC) Software could allow an unauthenticated, remote attacker to view system information that under normal circumstances should be prohibited. The vulnerability is due to incomplete input and validation checking mechanisms in the REST API URL request. An attacker could exploit this vulnerability by sending a malicious URL to the REST API. If successful, an exploit could allow the attacker to view sensitive system information. Cisco Bug IDs: CSCvg89442.
CVE-2018-0195	A vulnerability in the Cisco IOS XE Software REST API could allow an authenticated, remote attacker to bypass API authorization checks and use the API to perform privileged actions on an affected device. The vulnerability is due to insufficient authorization checks for requests that are sent to the REST API of the affected software. An attacker could exploit this vulnerability by sending a malicious request to an affected device via the REST API. A successful exploit could allow the attacker to selectively bypass authorization checks for the REST API of the affected software and use the API to perform privileged actions on an affected device. Cisco Bug IDs: CSCuz56428.
CVE-2018-0089	A vulnerability in the Policy and Charging Rules Function (PCRF) of Cisco Policy Suite (CPS) could allow an unauthenticated, remote attacker to access sensitive data. The attacker could conduct additional reconnaissance attacks. The attacker would also have to have access to the internal VLAN where CPS is deployed. The vulnerability is due to incorrect permissions of certain system files that is at rest. An attacker could exploit the vulnerability by using certain tools available on the internal network interface to request and view system files. An exploit could allow the at...

Will the vulnerable nodes be found?

Not will, only when and how fast is the question



The screenshot shows the Shodan Developer website. The navigation bar includes links for Dashboard, API Reference, Integrations, Pricing, and Contact Us. The main content area is titled "Introduction" and discusses the Exploits API, which provides access to several exploit/vulnerability data sources. A list of sources includes Exploit DB, Metasploit, and Common Vulnerabilities and Exposures (CVE). A button labeled "Next: REST API Documentation" is visible at the bottom of the page.

SHODAN DEVELOPER Dashboard API Reference Integrations Pricing Contact Us

API DOCUMENTATION

- Requirements
- Introduction
- Clients
- REST API Documentation
- Streaming API Documentation

EXPLOITS API DOCUMENTATION

- Introduction
- REST API Documentation

APPENDIX

Introduction

The Exploits API provides access to several exploit/ vulnerability data sources. At the moment, the API provides access to:

- Exploit DB
- Metasploit
- Common Vulnerabilities and Exposures (CVE)

If you have any data sources you would like to see in Shodan Exploits please contact us.

Next: REST API Documentation

REST API – Authentication vs Authorization?

Define operations in terms of HTTP methods

The HTTP protocol defines a number of methods used by most RESTful web APIs are:

- **GET** retrieves a representation of the resource.
- **POST** creates a new resource at the specified URI. The body of the request message provides the details of the new resource. Note that POST can also be used to trigger operations.
- **PUT** either creates or replaces the resource.
- **PATCH** performs a partial update of a resource. The request body specifies the set of changes to apply to the resource.
- **DELETE** removes the resource at the specified URI.

How does the SEPP know that all the requested info elements "make sense" for this TLS tunnel with this partner e.g. location, IMSI, keys

What elements would you allow your partners to create? Charging? New users?

Prepaid to postpaid? Malicious location "update"? Changing MSISDN? What replacements are ok? Code insertion?

Delete subscriber data?

And of course we get "normal" TLS security problems

Anonymous code signing certificates

COMODO

Trust: **basic**

Type: regular

Must gain a reputation to pass SmartScreen filter

SmartScreen reputation: **no**

\$299

BUY NOW

may not work for Tor users

thawte

Trust: **moderate**

Type: regular

Gains reputation faster than Comodo certificates

SmartScreen reputation: **no**

\$349

BUY NOW

may not work for Tor users

Symantec

Trust: **maximum**

Type: **EV certificate**

Contact us for purchase. USB token required (see FAQ)

SmartScreen reputation: **yes**

\$1599

CONTACT US

Code Signing FAQ

Anonymous EV SSL certificates

Get the Green Bar!

EV SSL certificate

Single domain (www. included)

2-4 business days

\$349

EV SSL + Code signing

Single domain + CS certificate

2-4 business days

\$599

EV SSL + EV Code signing

Single Domain + EV CS certificate

3-5 business days

\$1799

There is work to do....education on all sides

222.92.145.60 mail.ly.com

Database

◆◆3'◆yy◆ Telnet ◆◆◆◆◆◆◆◆

```
Pinging 222.92.145.60 with 32 bytes of data:
Reply from 222.92.145.60: bytes=32 time=310ms TTL=37
Reply from 222.92.145.60: bytes=32 time=310ms TTL=37
Reply from 222.92.145.60: bytes=32 time=302ms TTL=37
Reply from 222.92.145.60: bytes=32 time=298ms TTL=37

Ping statistics for 222.92.145.60:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 298ms, Maximum = 310ms, Average = 305ms
```

Osp:CMD NAME is too long! dwCmdlen=99

Username:fari/537.36

Password:

State][CollectOneAppState] Check App:ng-restapi State fail!

State][StateChangeNtfManager] ng-restapi state don't change! CurState:0

3306
tcp
mysql

MySQL Version: 5.7.14-log

5.7.14-log

5060
udp
sip

SIP/2.0 500 Internal Server Error

Via: SIP/2.0/UDP nm;rport=26810;received=83.119.29.102;branch=foo

Call-ID: 50000

From: <sip:nm@nm>;tag=root

To: <sip:nm2@nm2>;tag=foo

CSeq: 42 OPTIONS

Content-Length: 0

5269
tcp
xmpp

<stream:error><invalid-namespace xmlns='urn:ietf:params:xml:ns:xmpp-st

6379
tcp
redis

-NOAUTH Authentication required.

Pay attention to little details - configurations.....

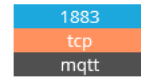
36.81.253.247

City	
Country	
Organization	
ISP	
Last Update	2018-06-01T06:31:29.820574
ASN	AS7713

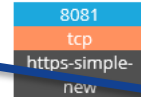
Ports



Services



MQTT Connection Code: 0
Topics:
/mne/alarm



HTTP/1.0 200 OK
Content-Type: application/json
Content-Length: 35
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: Content-Type, Authorization
Access-Control-Allow-Methods: GET, PUT, POST, DELETE, OPTIONS
Server: Werkzeug/0.12.2 Python/2.7.14
Date: Fri, 01 Jun 2018 06:30:45 GMT

the requested resource allows sharing with every origin. This basically means that any site can send an request and access the server's response

Supports info pulling, info putting and deletion

That is the software + version they use

They support RestAPI

```
{  
  "info": "REST API RestApi"  
}
```

New Risks Areas for Ongoing 5G Security Work

SBA Approach – New Thinking Required - Mindset / Business Realities

- Community have still “classical thinking”
 - Attack is focusing on air interface (UE – Network)
 - Core network is considered as one big trust zone (no network internal security zoning)
 - All NFVI’s in the SBA are part of that trust zone
- In real life:
 - Will all nodes connected to the “bus” be under full MNO control? Netflix “type”, new services e.g.auton. car
 - Will the “bus” cross network borders (e.g. for large operators) or cooperation with IT players
 - Test & trials e.g. for new services (debugging api)
 - Speed -> there will be no grace period for 5G
 - Preparedness (budget, incidence response plans, sec policy etc)

3GPP work still ongoing!!!!

Security

23,000 HTTPS certs will be axed in next 24 hours after private keys leak

Trustico, DigiCert come to blows as browsers prepare to snub Symantec-brand SSL

By [John Leyden](#) 1 Mar 2018 at 00:43

61 [SHARE](#) ▼

Critical flaw in Pivotal's Spring Data REST allows to hack any machine that runs an application built on its components

March 5, 2018 By [Pierluigi Paganini](#)

[My Page](#) [Like 27](#)

A critical flaw in Pivotal's Spring Data REST allows remote attackers to execute arbitrary commands on any machine that runs an application built using its components.

Bell Labs

Evolution of protection

Many shades of grey

- Learn from IT Security
 - They deal constantly with attacks
 - They know how to automate
- Black and white is too coarse for 5G
- Operators know their partners

- Scoring (partner, parameters, routing)
 - The suspicious
 - Learn your partners "fingerprint"
 - The bad
 - Know how a bad data request looks like
 - And the really bad
 - Identify "bad payload"



Summary

All networks are attacked, but not are equally vulnerable

- 5G the security race will be on when core network nodes are out
- Duty of the whole industry
- Security plans are essential, you will be under attack
- 3GPP SA3 & GSMA DESS will do their best to protect the data, but authorization depends on each operator (who do you trust and how far can you trust each message?)
- Need a fine grained authorization control based on suspiciousness
- The biggest security risks don't come from general security risks, but from combination of being blue-eyed, business pressure & customization

Thanks to
EU SCOTT Project for funding part of this research

Questions?

Silke.Holtmanns@nokia.com