



SAP's NETWORK PROTOCOLS REVISITED

MARTIN GALLO

MARCH 2014



AGENDA

SAP SECURITY

NETWORK PENETRATION TESTING

THIS TALK

APPROACH

TOOLS

CLASSIC SAP ENV

SAP ROUTER

SAP GATEWAY/RFC

SAP DISPATCHER/DIAG

SAP MESSAGE SERVER

SAP ENQUEUE SERVER

MODERN SAP ENV

SAP NW GATEWAY

SAP HANA

DISCOVERY & INFO GATHERING

VULN ASSESSMENT & EXPLOITATION

DEFENSE

CONCLUSIONS

SAP SECURITY

+ INFO

+ TOOLS

+ STANDARDS

+ RESEARCH

+ COMPANIES

+ MEDIA ATTENTION

SAP SECURITY

- NON-SPECIALISTS
- MOST ON APP LAYER
- STEEP LEARNING CURVE
- NON-TARGETED PENTEST
- MEDIA ATTENTION

NETWORK PENETRATION TESTING

DISCOVERY
INFO GATHERING
VULN ASSESSMENT
EXPLOITATION
POST-EXPLOITATION

NETWORK PENETRATION TESTING

ON A SAP ENV?

THIS TALK

OLD & NEW
EXCLUDED WEB
NOT ALL COVERED
NOT A PENTEST GUIDE

APPROACH

BLACK-BOX
WORK IN PROGRESS
INCREMENTAL LEARNING
RELY ON OTHER'S WORK
NOT COMPLETE ACCURATE

TOOLS

pysap

PYTHON LIBRARY

CRAFT PACKETS

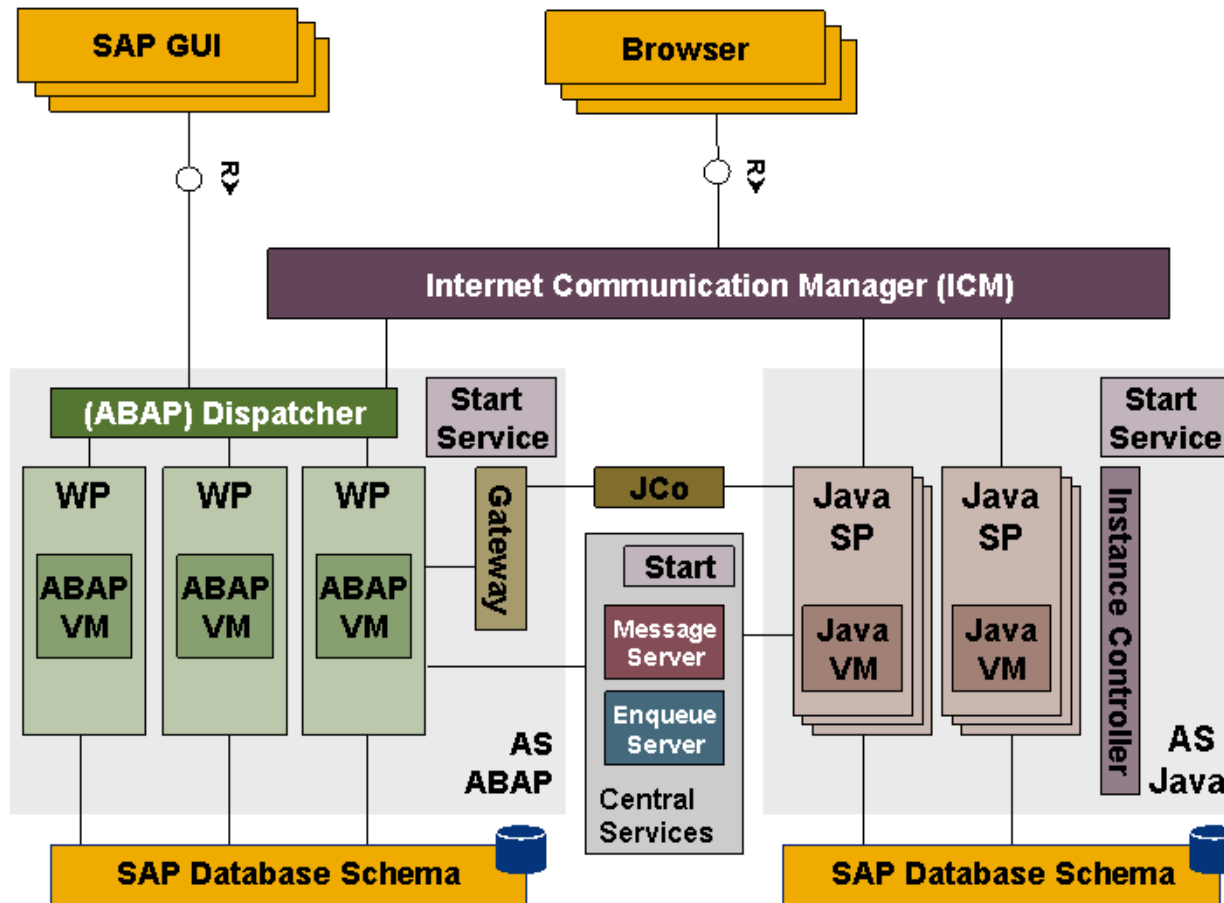
WIRESHARK PLUGIN

DISSECT SAP PROTOCOLS

[pysap](#)

[Wireshark plugin](#)

CLASSIC SAP ENV



CLASSIC SAP ENV

SAP ROUTER

SAP GATEWAY/RFC

SAP DISPATCHER/DIAG

SAP MESSAGE SERVER

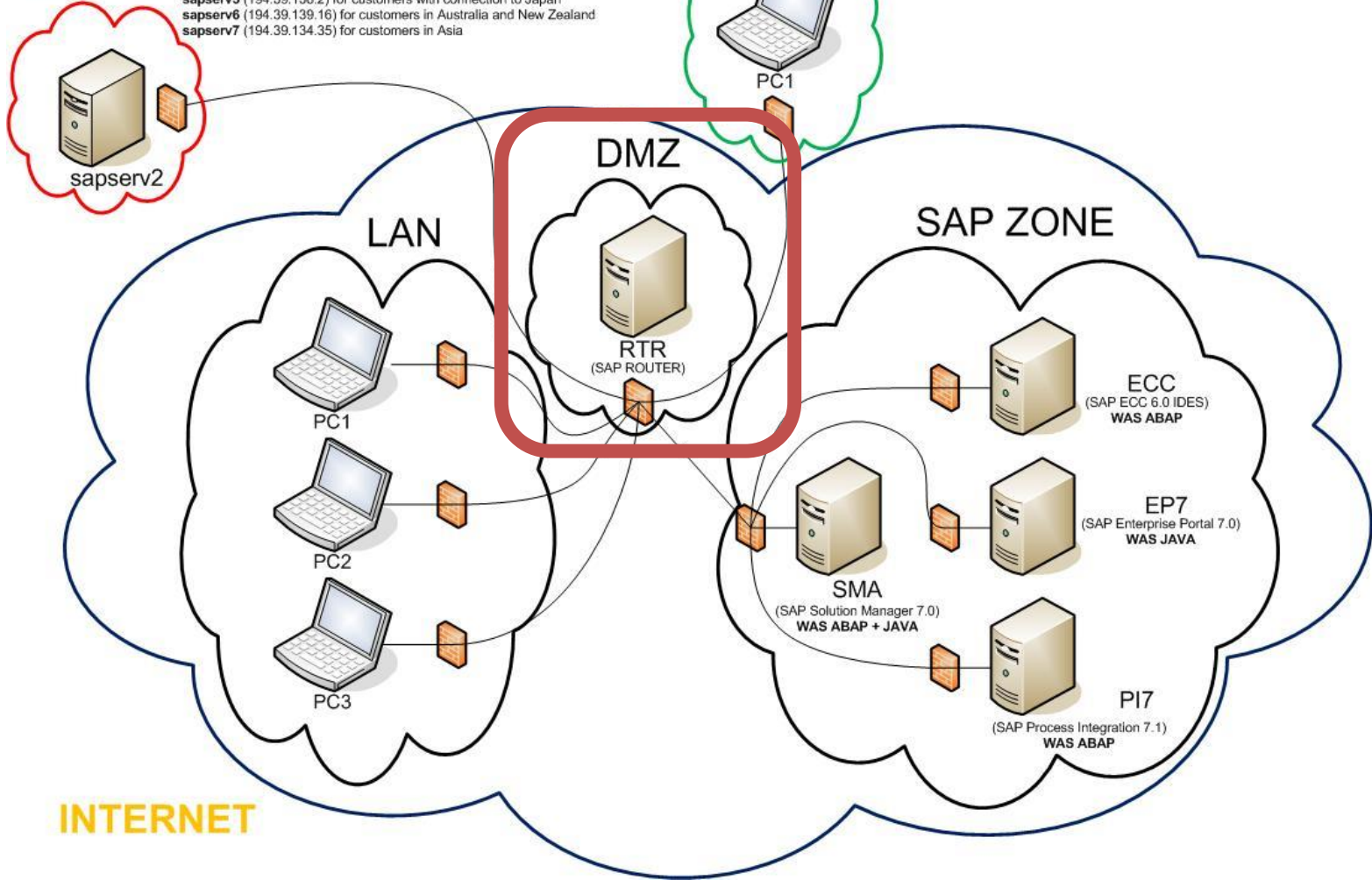
SAP ENQUEUE SERVER

SAP ROUTER

APPLICATION LEVEL-GATEWAY
REVERSE PROXY
STAND ALONE APP
ON ALL SAPs INSTALLATIONS
UNENCRYPTED BY DEFAULT
INTERNET EXPOSED

SAP AG

sapserv1 (194.117.106.129) connection via Internet VPN
sapserv2 (194.39.131.34) connection via Internet SNC
sapserv3 (147.204.2.5) for customers with connection to Germany
sapserv4 (204.79.199.2) for customers in America
sapserv5 (194.39.138.2) for customers with connection to Japan
sapserv6 (194.39.139.16) for customers in Australia and New Zealand
sapserv7 (194.39.134.35) for customers in Asia



SAP ROUTER

WELL-KNOWN ATTACKS:

INFO REQUEST

USE AS A PROXY

SNIFF ROUTE/PASSWORDS

SCAN INTERNAL NETWORKS

[Mariano's talk at HITB 2010](#)

[Dave's SAP Smashing blog post](#)

SAP ROUTER

LOOKING INSIDE:

ADMIN PACKETS
CONTROL MESSAGES
ERROR INFORMATION
ROUTE REQUEST
PONG

SAP ROUTER

ADMIN PACKETS:

REMOTE ADMINISTRATION
FOUND UNDOCUMENTED

COMMANDS: SET/CLEAR PEER TRACE,
TRACE CONNECTION

SAP ROUTER

CONTROL MESSAGES:

INTERNAL CONTROL

UNDOCUMENTED OPCODES:

VERSION REQUEST/REPOSE, SET
HANDLE, SNC REQUEST/ACK

SAP ROUTER

ROUTE REQUEST:

ROUTE STRING

LIST OF ROUTING HOPS

PASSWORD PROTECTED (OPTIONAL)

SAP ROUTER

RECENT ATTACKS:

INFO DISCLOSURE
ROUTE STRING HEAP OVERFLOW

[ERPScan's DSECRG-13-013 advisory](#)
SAP Security Notes [1820666](#) / [1663732](#)

SAP ROUTER

SECURITY MEASURES:

PATCH

ENFORCE SNC USE

HARDEN ROUTE TABLE

PUT BEHIND FIREWALL

DON'T USE PASSWORDS

SAP GATEWAY/RFC

RFC INTERFACE
INTEGRATION W/EXT SERVERS
UNENCRYPTED BY DEFAULT
GENERALLY EXPOSED

SAP GATEWAY/RFC

WELL-KNOWN ATTACKS:

INFO GATHERING
MONITOR MODE
MITM / SNIFFING
SOME RCE VULNS

[Mariano's Attacking the Giants talk at BlackHat and Deepsec 2007](#)
and [SAP Penetration Testing talk at BlackHat 2009](#)

SAP GATEWAY/RFC

WELL-KNOWN ATTACKS:

LOGIN BRUTE-FORCE
+ TONS OF ATTACKS ON RFCs
RFC EXEC, SAPXPG,
CALLBACK, EVIL TWIN, ...

[Mariano's Attacking the Giants talk at BlackHat and Deepsec 2007](#)
and [SAP Penetration Testing talk at BlackHat 2009](#)

SAP GATEWAY/RFC

LOOKING INSIDE:

MAIN PACKETS

MONITOR PACKETS

RFC TABLES

SAP GATEWAY/RFC

SECURITY MEASURES:

PATCH (CLIENT/SERVER)

USE ACLs

DISABLE MONITOR

ENFORCE SNC USE

ENABLE (AND REVIEW) LOGS

[Security Settings in the SAP Gateway](#)

SAP DISPATCHER/DIAG

COMM BETWEEN GUI/APP SERVER
RFC EMBEDDED CALLS
ONLY COMPRESSED
UNENCRYPTED BY DEFAULT

SAP DISPATCHER/DIAG

WELL-KNOWN ATTACKS:

ATTACKS ON GUI CLIENTS
SNIFFING LOGIN CREDENTIALS

[Secaron's sniffing paper](#)

[Ian's Talk at 44con 2011](#)

[Andrea's Talk at Troopers 2011](#)

SAP DISPATCHER/DIAG

RECENT ATTACKS:

INFO GATHERING

LOGIN BRUTE-FORCE

ROGUE SERVER + GUI SHORTCUT

BUFFER OVERFLOWS (W/TRACE ON)

[Talk at Defcon 20/Brucon 2012](#)
[CORE-2012-0123 Advisory](#)

SAP DISPATCHER/DIAG

SECURITY MEASURES:

PATCH (SERVER / GUI)
ENFORCE SNC USE

SAP MESSAGE SERVER

ONE PER SYSTEM
LOAD BALANCING FOR GUI/RFC
INTERNAL COMM W/APP SERVERS
INT/EXT TCP PORT + HTTP

SAP MESSAGE SERVER

WELL-KNOWN ATTACKS:

MONITOR MODE

INFO GATHERING (HOW?)

IMPERSONATE APP SERVER (HOW?)

OLD BUFFER OVERFLOWS ON HTTP

SAP MESSAGE SERVER

LOOKING INSIDE:

MAIN PACKETS

ADM PACKETS

~ 60 ADMIN OPCODES

~ 75 REGULAR OPCODES

SAP MESSAGE SERVER

LOOKING INSIDE:

DUMP DATA

MONITOR CLIENTS

SEND/RECV MESSAGES

CHANGE CONFIG PARAM

SAP MESSAGE SERVER

RECENT ATTACKS:

MS BUFFER OVERFLOWS

[ZDI-12-104/111/112](#) Advisories
SAP Security Notes [1649838](#) / [1649840](#)

SAP MESSAGE SERVER



RECENT ATTACKS:



MS MEMORY CORRUPTION

GIVE CONN ADMIN PRIVS
OVERWRITE CHANGE PARAM FUNCTION POINTER
SEND CHANGE PARAM WITH PAYLOAD
PWN

[CORE-2012-1128 Advisory](#)
[SAP Security Note 1800603](#)

SAP MESSAGE SERVER

NEW/OLD ATTACKS:

IMPERSONATE APP SERVER

SAP MESSAGE SERVER

ACCESS LEVEL:

	EXTERNAL PORT	INTERNAL PORT	MONITOR MODE
MONITOR CLIENTS	X		
MS BUFFER OVERFLOW	X	X	
MS MEMORY CORRUPTION	X	X	
DUMP DATA		X	
IMPERSONATE APP SERVER		X	
CHANGE PARAM		X	X

SAP MESSAGE SERVER

SECURITY MEASURES:

PATCH

USE ACLs

DISABLE MONITOR

SEPARATE INT/EXT PORT

ENABLE (AND REVIEW) LOGS

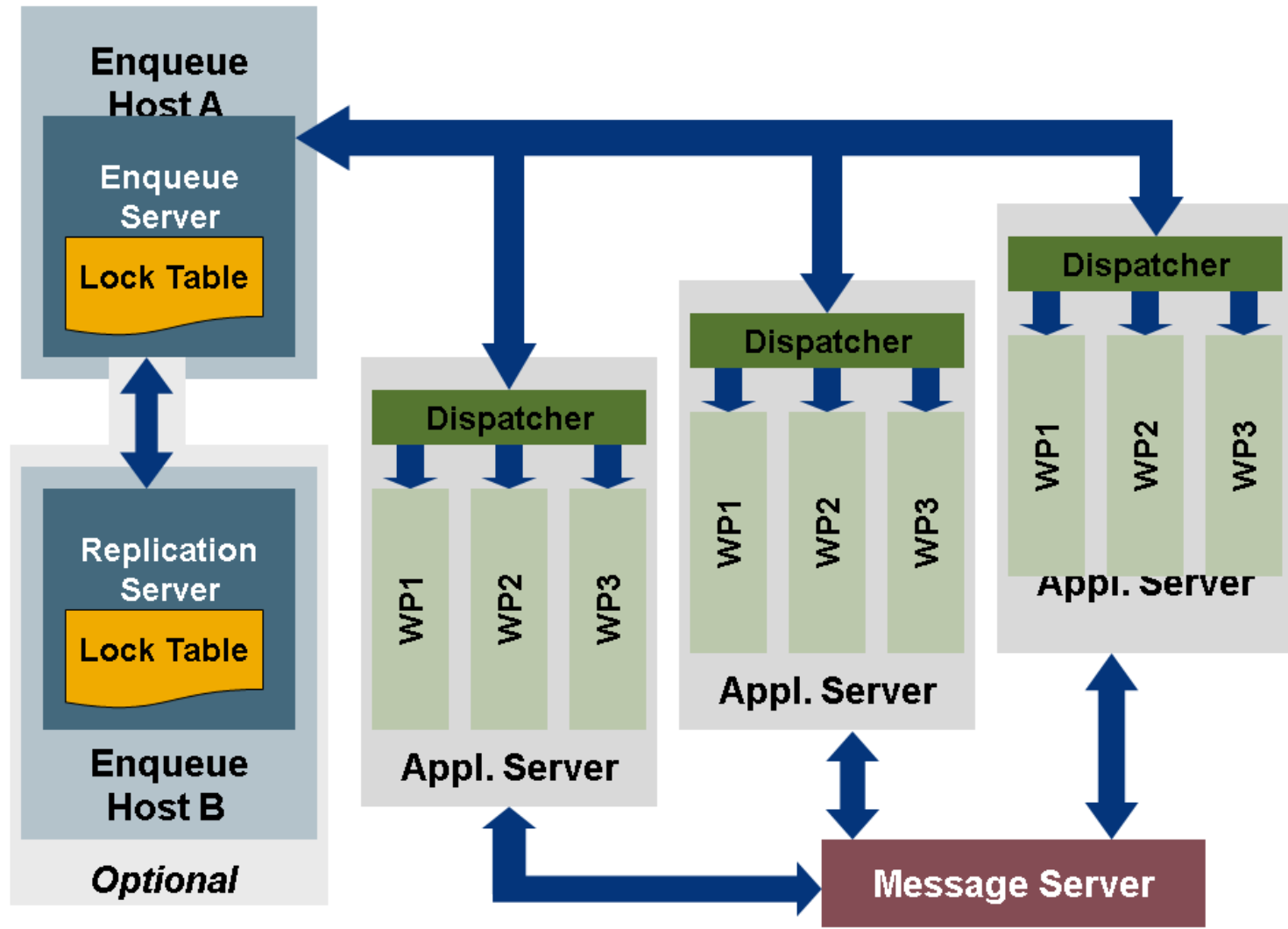
[Security Settings for the SAP Message Server](#)

[SAP Security Note 821875](#)

SAP ENQUEUE SERVER

ONE PER SYSTEM
LOCK MECHANISM

CAN RUN STANDALONE
REPLICATION SERVER FOR HA



SAP ENQUEUE SERVER

WELL-KNOWN ATTACKS:

???

SERVER CRASHES (???)

TRANSFER FILES (???)

SAP Security Notes [948457](#) / [959877](#)

SAP ENQUEUE SERVER

LOOKING INSIDE:

CONNECTION ADMIN
SERVER ADMIN
REPLICATION
STATS

SAP ENQUEUE SERVER

SECURITY MEASURES:

PATCH

USE ACLs

ENABLE (AND REVIEW) LOGS

RESTRICT ACCESS TO THE SERVICE

(NO SNC SUPPORTED?)

SAP Security Notes [1879601](#) / [1495075](#)

CLASSIC SAP ENV

~~SAP ROUTER~~

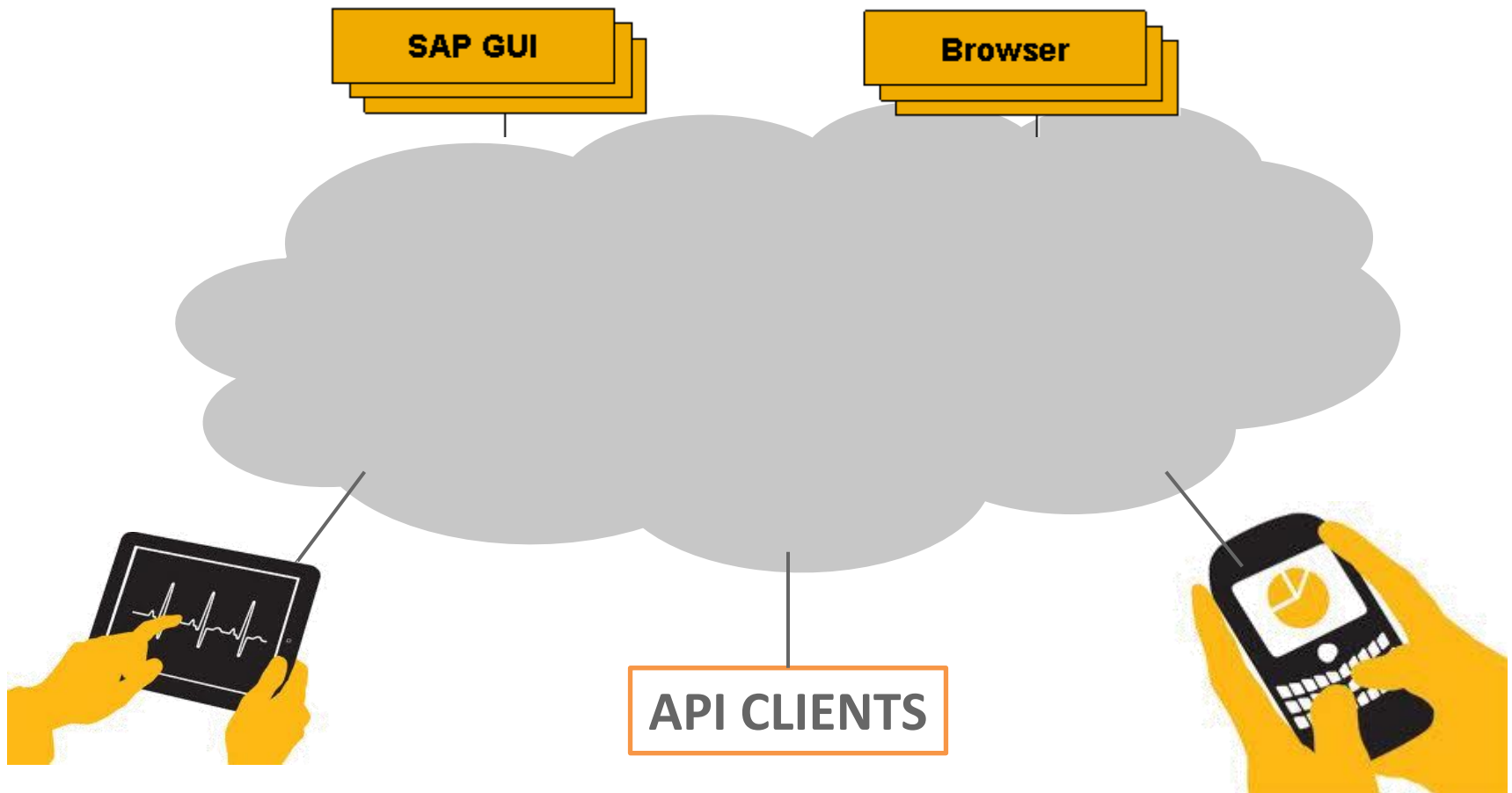
~~SAP GATEWAY/RFC~~

~~SAP DISPATCHER/DIAG~~

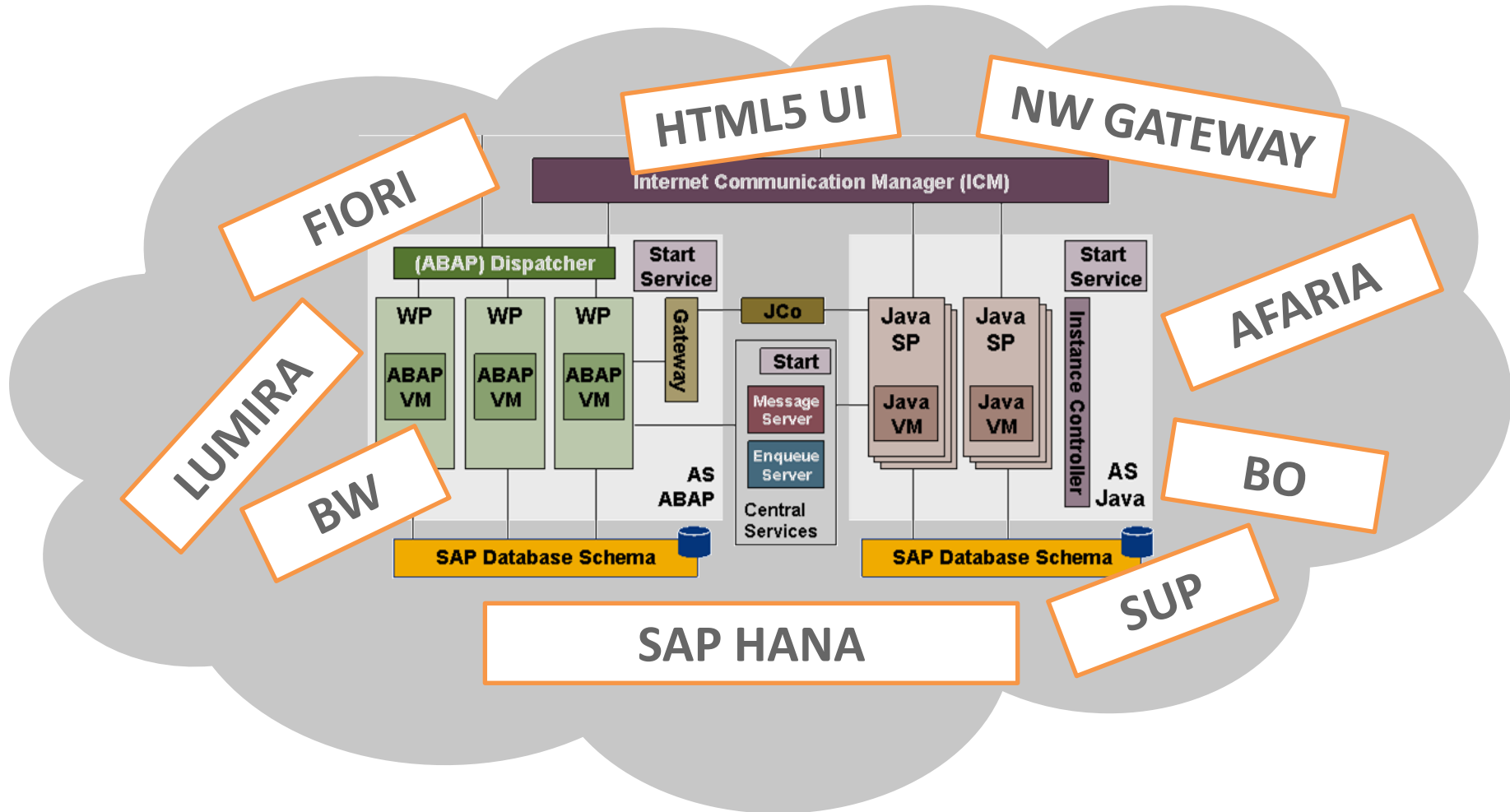
~~SAP MESSAGE SERVER~~

~~SAP ENQUEUE SERVER~~

MODERN SAP ENV



MODERN SAP ENV



MODERN SAP ENV

SAP NETWEAVER GATEWAY
SAP HANA

SAP NW GATEWAY

REST API
INTEGRATION
ODATA/ATOM PROTOCOLS
ADD-ON FOR SAP NW ABAP

OData

SAP Netweaver Gateway and Odata

SAP HANA

IN-MEMORY DATABASE
PROTOCOL SPEC AVAILABLE

[SAP HANA SQL Command Network Protocol](#)

DISCOVERY & INFO GATHERING

SERVICE DISCOVERY

INFO DISCLOSURE

BRUTE FORCE ON AUTH SERVICES

VULN ASSESSMENT & EXPLOITATION

SNIFF/MITM

INVOLVE CLIENTS

ABUSE FUNCTIONS

SEVERAL RCE VULNS

REACH PRIVILEGE CONNECTION

SERVICE / PROTOCOL

**DISCOVERY & INFO
GATHERING**

**VULN ASSESS &
EXPLOITATION**

ROUTER

INFO REQUEST
~~INFO DISCLOSURE~~
INTERNAL NETWORK SCAN

SNIFF
PROXY
~~HEAP OVERFLOW~~

GATEWAY/RFC

INFO
BRUTE FORCE

~~RCE~~
SNIFF
MONITOR
RFC ATTACKS

DISPATCHER/DIAG

INFO
BRUTE FORCE

~~RCE~~
SNIFF
ROGUE SERVER
ATTACK GUI USERS

MESSAGE SERVER

DUMP DATA
MONITOR APP SERVERS

~~RCE~~
MONITOR
IMPERSONATE
~~BUFF OVERFLOW~~
~~MEMORY CORRUPTION~~

ENQUEUE SERVER

INFO

TRANSFER FILES
SERVER CRASHES
???

DEFENSE

TEST, TEST AND TEST
PATCH, PATCH AND PATCH
USE ENCRYPTED CHANNELS
ENABLE AND MONITOR LOGS
RESTRICT ACLs ON ALL SERVICES

CONCLUSIONS

NEW & RECENT ATTACKS
OLD ATTACKS PRACTICAL
DEFENSE & HARDENING
MORE PROTOCOL'S DETAILS



Q&A

Thank you !
mgallo@coresecurity.com

Thanks to
Diego, Sebas, Ivan, Francisco, Dana and Euge

Cover photo © [Marcelo Schiavon](#)

UPDATED TOOLS

pysap & wireshark plugin v0.1.4

+ PROTOCOLS

+ EXAMPLES

+ IMPROVEMENTS & FIXES

THANKS JORIS, FLORIAN, DAVE, DANIEL & ARNOLD
FOR VALUABLE FEEDBACK AND BUG REPORTS

[pysap](#)

[Wireshark plugin](#)

UPDATED TOOLS

pysap & wireshark plugin v0.1.4

STILL NEED WORK ON:

BUGFIXES AND TEST

IMPROVE: RFC, DIAG

NEW PROTOCOLS: P4? HANA?

MORE EXAMPLES AND ATTACKS

SUPPORT FOR + SAP GUI/NW VERSIONS

[pysap](#)

[Wireshark plugin](#)

UPDATED TOOLS



NMAP SERVICE DISCOVERY

IMPROVED/ADDED SERVICE PROBES FOR
THE SERVICES REVIEWED:

SAPROUTER, DISPATCHER/DIAG, MS,
ENQUEUE, GW/RFC