

Uncovering SAP vulnerabilities: Reversing and breaking the Diag protocol

Martin Gallo – Core Security
Defcon 20 – July 2012

Agenda

- Introduction
- Motivation and related work
- SAP Netweaver architecture and protocols layout
- Dissecting and understanding the Diag protocol
- Results and findings
- Defenses and countermeasures
- Conclusion and future work

Introduction

Introduction

- Leader business software provider
- Sensitive enterprise business processes runs on SAP systems
- SAP security became a hot topic
- Some components still not well covered
- Proprietary protocols used at different components

Introduction

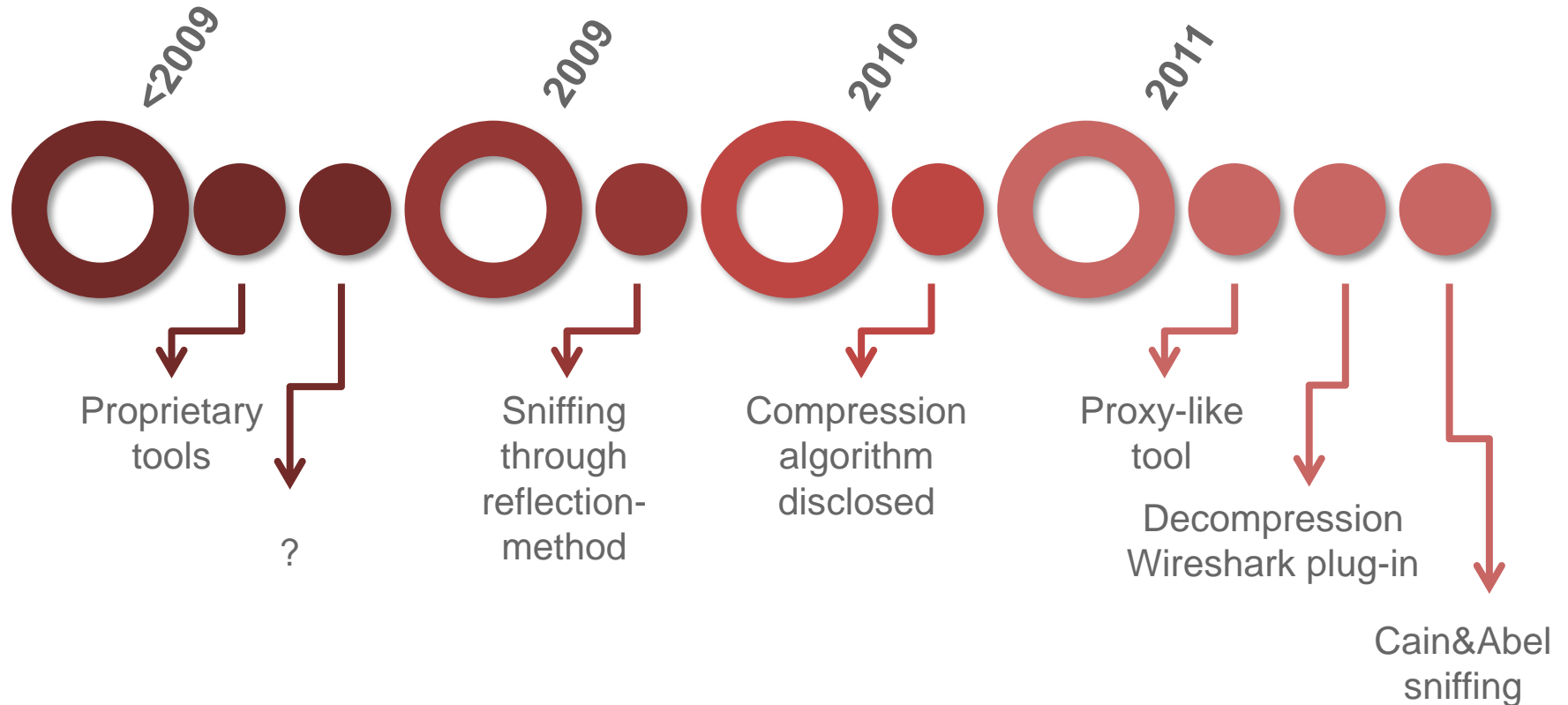
- Dynamic Information and Action Gateway (Diag) protocol (aka “SAP GUI protocol”)
- Link between presentation layer (SAP GUI) and application layer (SAP Netweaver)
- Present in every SAP NW ABAP AS
- Compressed but unencrypted by default
- TCP ports 3200 to 3298

Agenda

- Introduction
- Motivation and related work
- SAP Netweaver architecture and protocols layout
- Dissecting and understanding the Diag protocol
- Results and findings
- Defenses and countermeasures
- Conclusion and future work

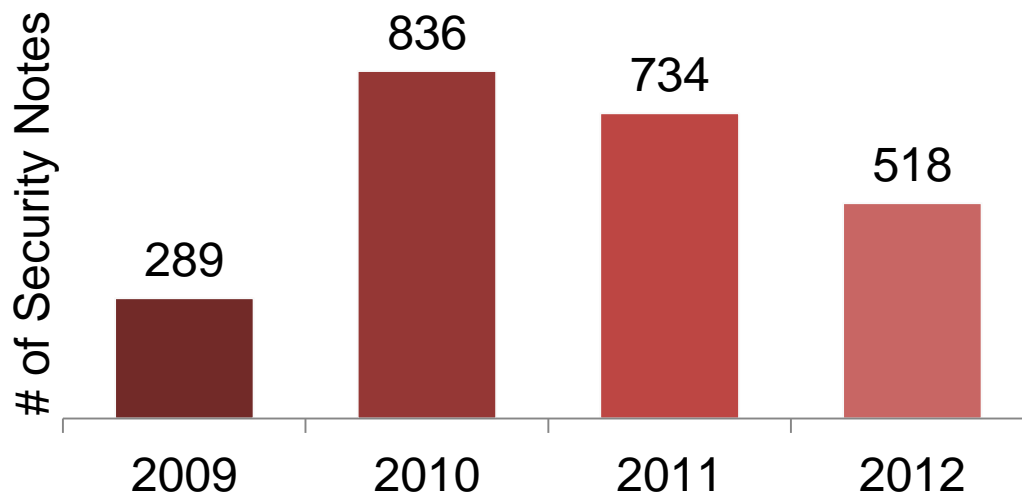
Motivation and related work

Previous work on Diag protocol



Motivation

- Previous work mostly focused on decompression
- Protocol inner workings remains unknown
- No practical tool for penetration testing



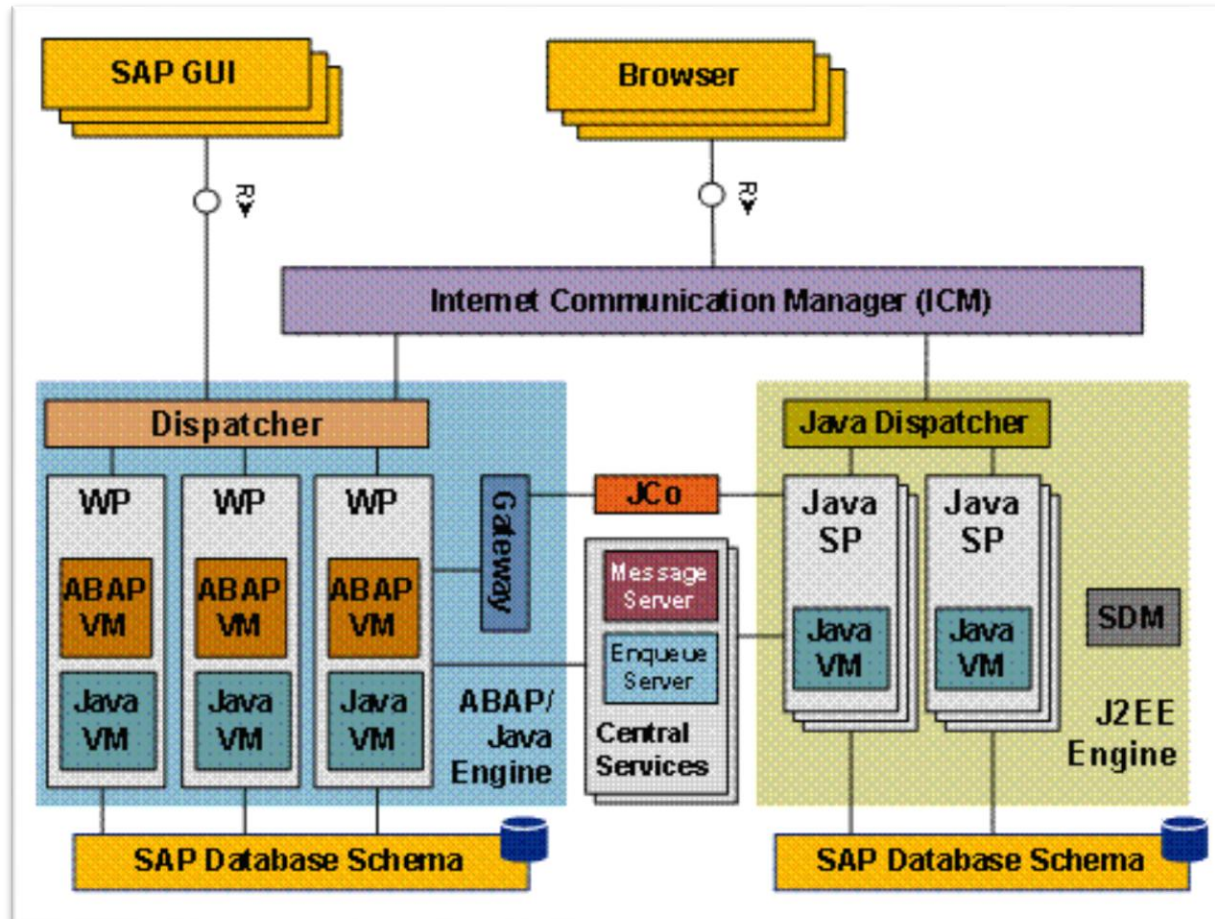
Only 2 out of ~2300 security fixes published by SAP since 2009 affected components related to Diag

Agenda

- Introduction
- Motivation and related work
- SAP Netweaver architecture and protocols layout
- Dissecting and understanding the Diag protocol
- Results and findings
- Defenses and countermeasures
- Conclusion and future work

SAP Netweaver architecture and protocols layout

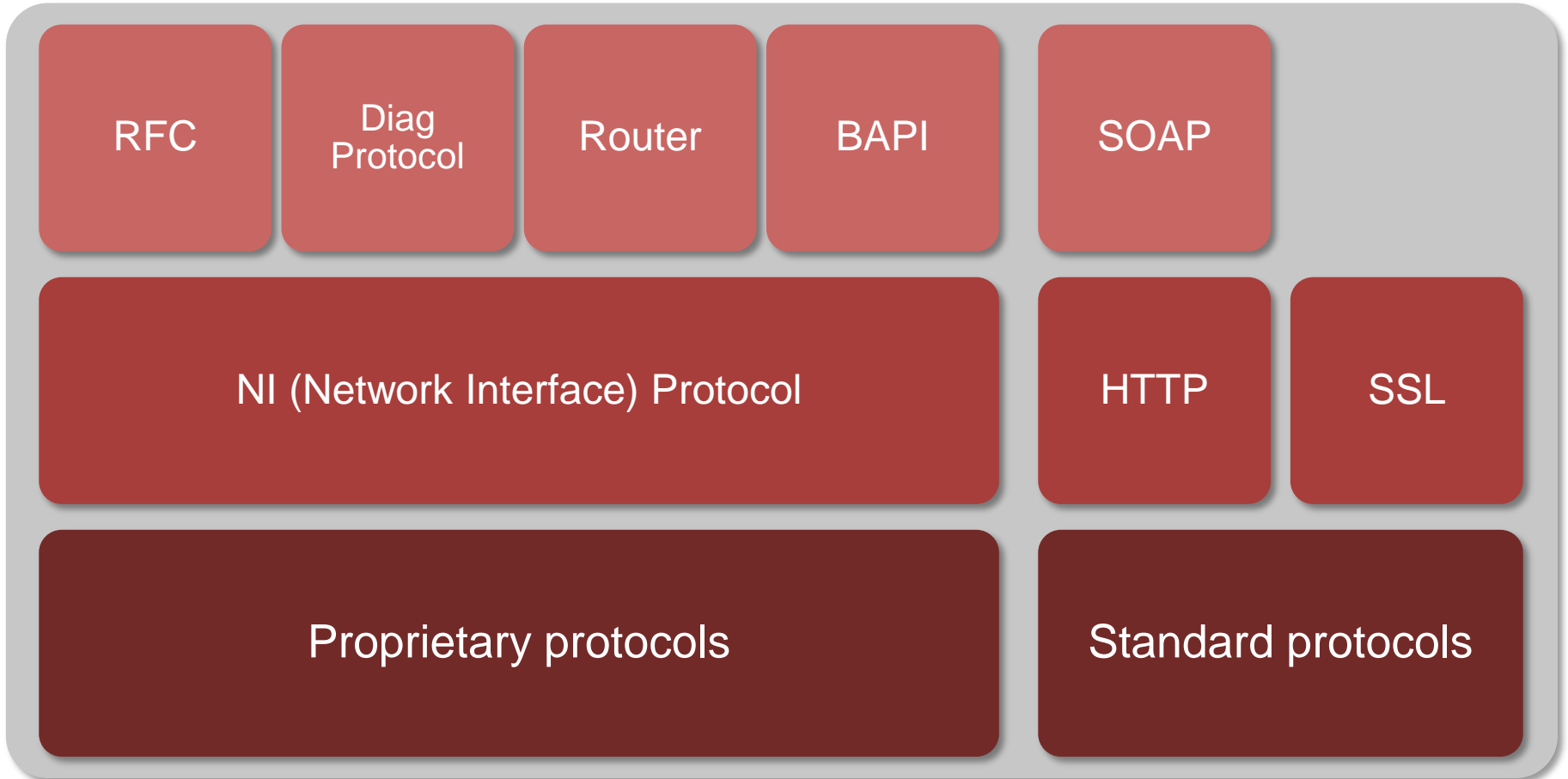
SAP Netweaver architecture



Relevant concepts and components

- ABAP
 - SAP's programming language
- Dispatcher and work processes (wp)
 - **Dispatcher**: distribute user requests across wp
 - **Work processes**: handles specific tasks
 - Types: **dialog**, spool, update, background, lock
- Dialog processing
 - Programming method used by ABAP
 - Separates business programs in *screens* and *dialog steps*

SAP Protocols layout



Agenda

- Introduction
- Motivation and related work
- SAP Netweaver architecture and protocols layout
- Dissecting and understanding the Diag protocol
- Results and findings
- Defenses and countermeasures
- Conclusion and future work

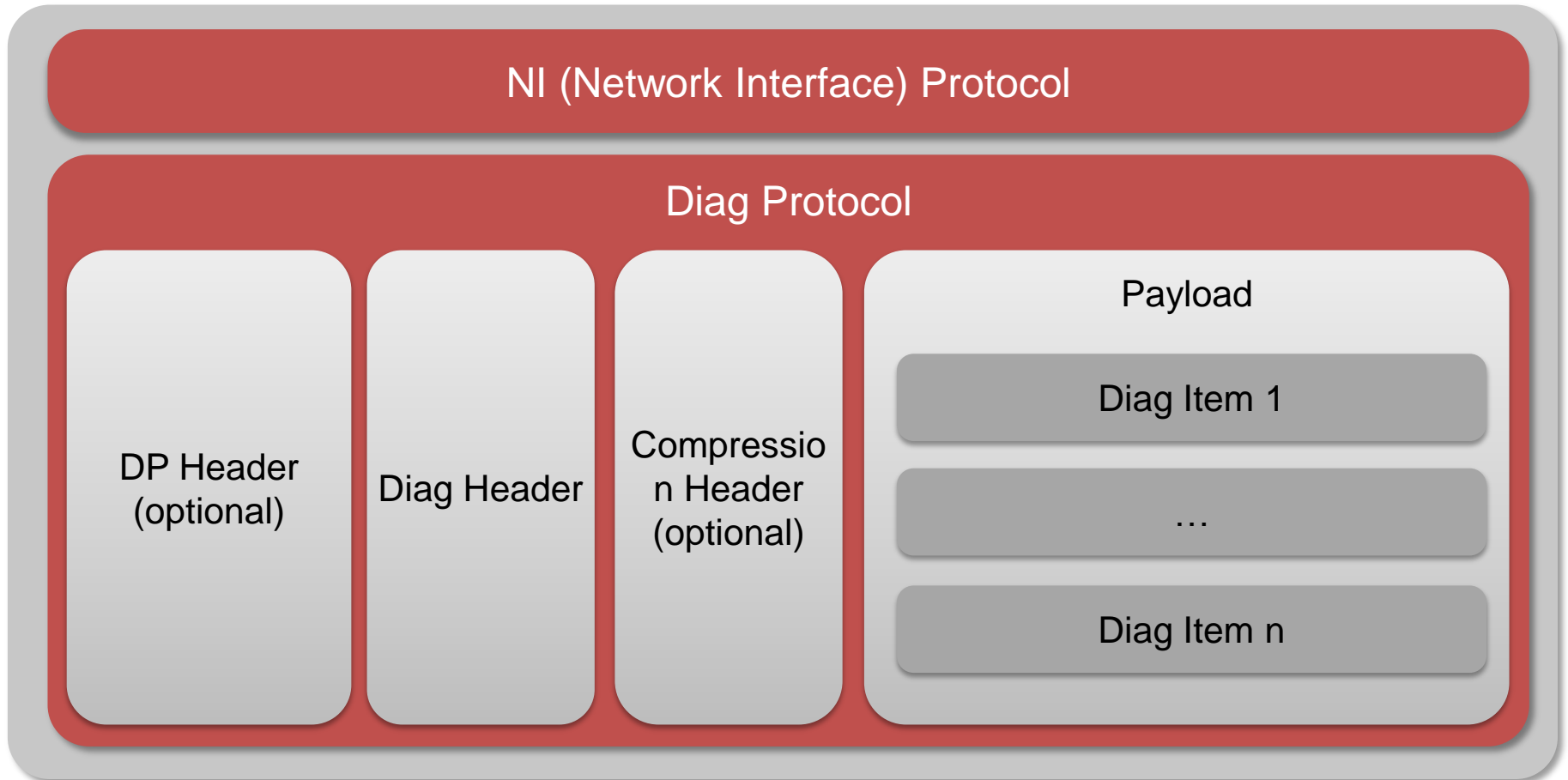
Dissecting and understanding the Diag protocol

Dissecting and understanding the Diag protocol

Approach

- 'Black-box'
- No binary reverse engineering techniques were used
- Enable system/developer traces (GUI/app server)
- Analyze network and application traces
- Learn by interacting with the components (GUI/app server)
- Continuous improvement of test tools based on gained knowledge

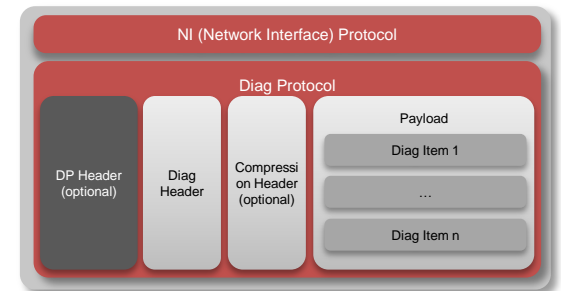
Dissecting and understanding the Diag protocol



Dissecting and understanding the Diag protocol

Initialization

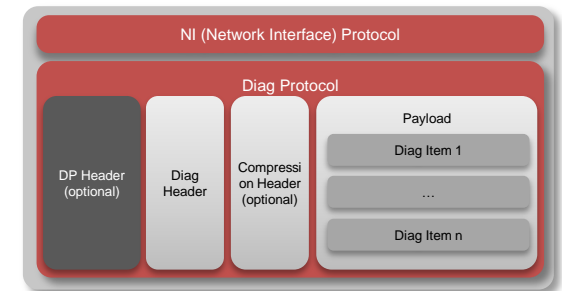
- Identified only two relevant protocol states:
 - Not initialized
 - Initialized
 - User's context assigned in shared memory
- Started by GUI application
- Only first packet
- Always uncompressed



Dissecting and understanding the Diag protocol

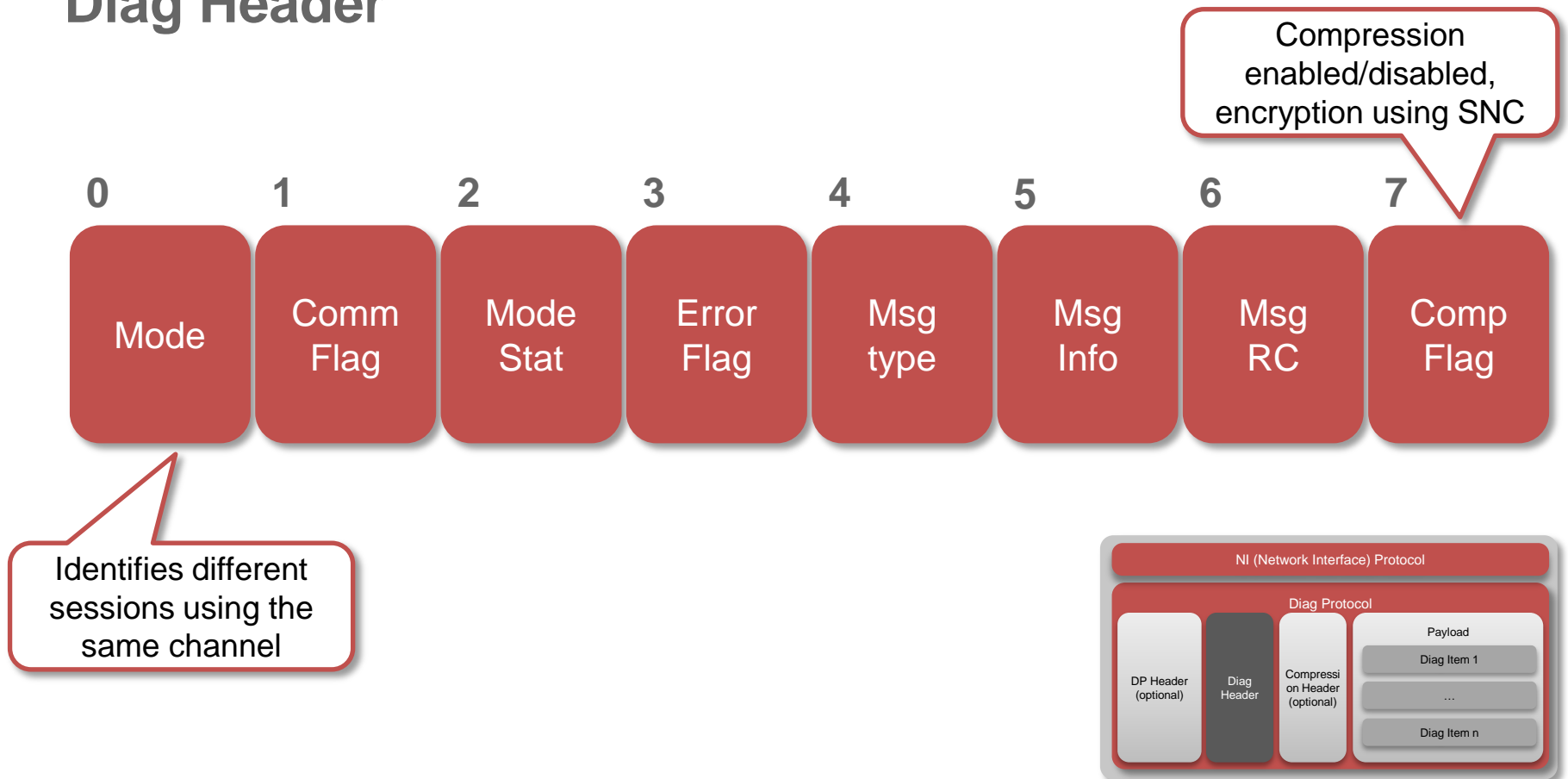
DP Header

- 200 bytes length
- Two different semantics
 - **IPC (inter process communication)**
 - Used in communications between dispatcher and work processes
 - Synchronization and status
 - **Network**
 - Most fields filled with default values
 - Relevant fields:
 - Terminal name, Length
- Only present during initialization (first packet)



Dissecting and understanding the Diag protocol

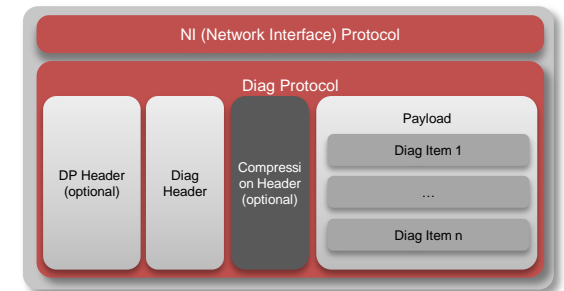
Diag Header



Dissecting and understanding the Diag protocol

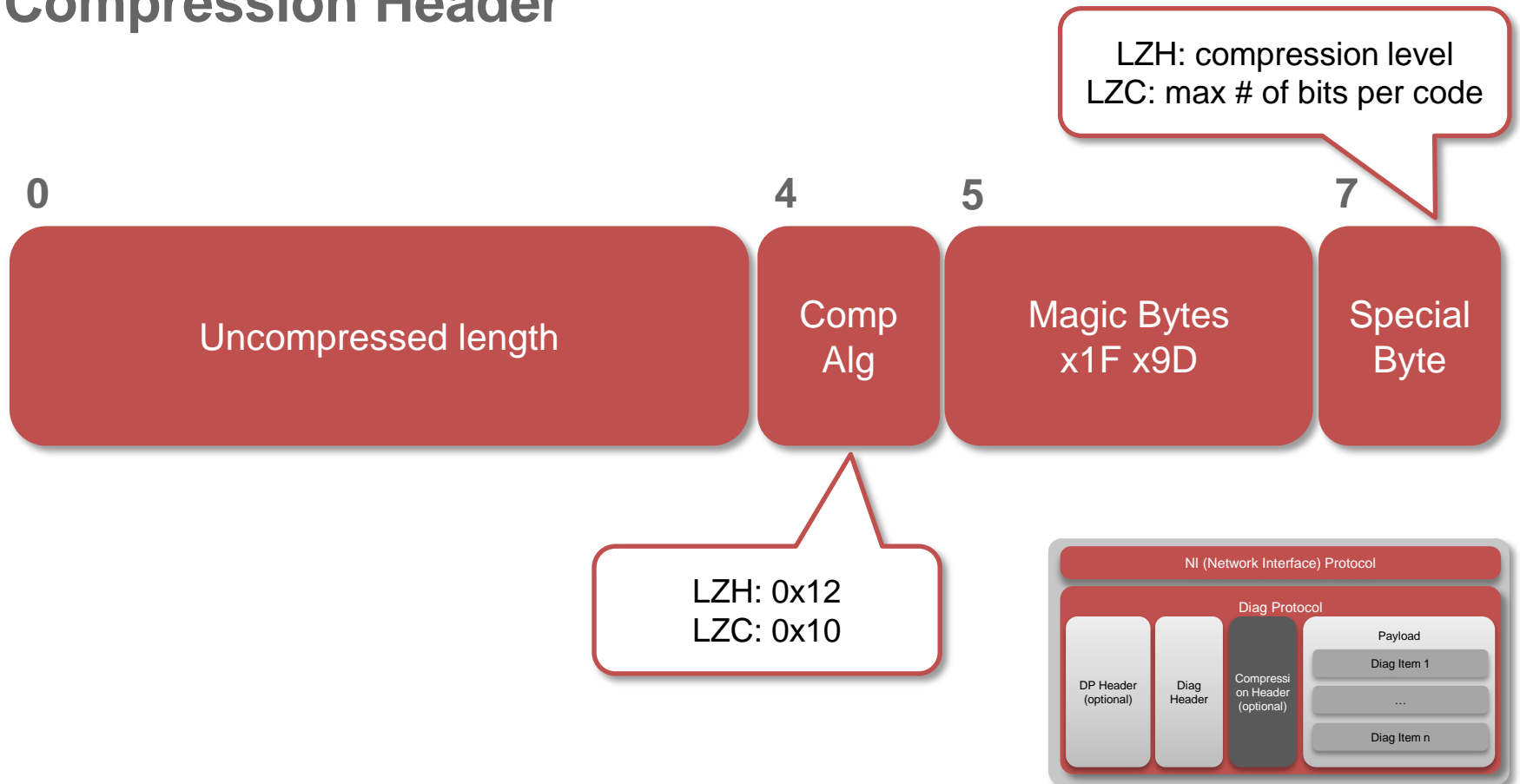
Compression

- Enabled by default
- Uses two variants of *Lempel-Ziv Adaptive Compression Algorithm*
 - *LZH* (Lempel-Ziv-Huffman) LZ77
 - *LZC* (Lempel-Ziv-Welch-Thomas) LZ78
- Same implementation as *SAP's MaxDB* open source project
- Can be disabled in GUI by setting *TDW_NOCOMPRESS* environment variable



Dissecting and understanding the Diag protocol

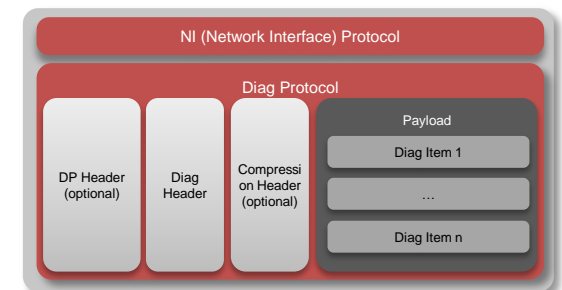
Compression Header



Dissecting and understanding the Diag protocol

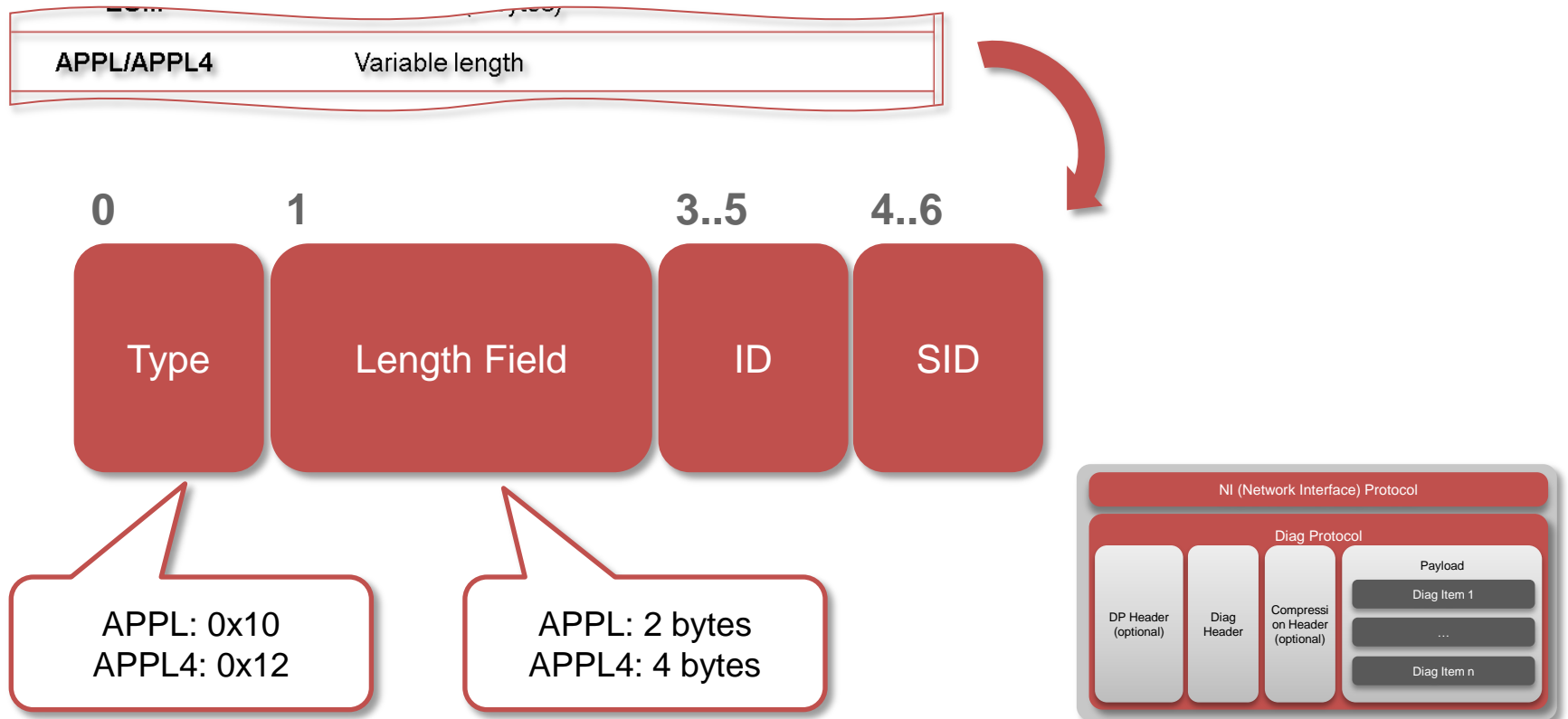
Payload

SES	Fixed length (16 bytes)	Session information
ICO	Fixed length (20 bytes)	Icon information
TIT	Fixed length (3 bytes)	Title information
DiagMessage	Fixed length (76 bytes)	Old Diag message
OKC	(? Bytes)	
CHL	Fixed length (22 bytes)	
SBA	Fixed length (9 bytes)	List items
EOM	Fixed length (0 bytes)	End of message
APPL/APPL4	Variable length	
DIAG_XMLBlob	Variable length	XML Blob
SBA2	Fixed length (36 bytes)	List items



Dissecting and understanding the Diag protocol

APPL/APPL4 items



Diag protocol security highlights

Protocol version

- APPL item included in payload during initialization
- Can disable compression using version number “200”

Authentication

- Performed as a regular dialog step
- Set user’s context on work processes shared memory

Embedded RFC calls

- APPL item that carries RFC calls in both directions
- Server doesn’t accept RFC calls until authenticated

Agenda

- Introduction
- Motivation and related work
- SAP Netweaver architecture and protocols layout
- Dissecting and understanding the Diag protocol
- Results and findings
- Defenses and countermeasures
- Conclusion and future work

Results and findings

Packet dissection

- Wireshark plug-in written in C/C++
 - NI Protocol dissector
 - TCP reassembling
 - Router Protocol dissector
 - Basic support
 - Diag protocol dissector
 - Decompression
 - DP header / Diag Header / Compression Header
 - Item ID/SID identification and dissection of relevant items
 - Call RFC dissector for embedded calls
 - RFC protocol dissector
 - Basic coverage of relevant parts



Packet dissection

Wireshark 1.9.0 (SVN Rev 43678 from /trunk) on ubuntu-gui702

Filter: **sapdiag** Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
110	134.664006000	10.0.0.4	10.0.0.103	SAPDIAG	391 Uncompressed Length=439	
111	134.672241000	10.0.0.103	10.0.0.4	SAPDIAG	659 Uncompressed Length=1051	

▼ SAP NI Protocol, Len: 589

▼ SAP Diag Protocol, Uncompressed Len: 1051

- Header
 - Mode: 0
 - Com Flag: 0x00
 - Mode Stat: 17
 - Error Flag: False
 - Message Type: 0
 - Message Info: 1
 - Message Rc: 0
 - Compress: Compression switched on (0x01)
- Compression Header
 - Uncompressed Length: 1051
 - Compression Algorithm: LZH (0x12)
 - Magic Bytes: 0x1f9d
 - Special: 0x02

0000 10 06 11 00 20 ff 7f fe 2d d8 b7 37 d6 74 08 7e
0010 13 05 97 15 97 eb f2 3f 8d 03 70 ff 0f 00 00 00
0020 00 00 00 00 00 10 06 23 00 0f 00 00 10 0e 01 34
0030 21 21 20 00 ff 54 46 28 00 10 06 27 00 20 00 00

Frame (659 bytes) Uncompressed Data (1051 bytes)

Frame (frame), 659 bytes Profile: Def

111 134.672241000 10.0.0.103 10.0.0.4 SAPDIAG 659 Uncompressed Length=1051 (on ubuntu-gui702)

▼ SAP NI Protocol, Len: 589

▼ SAP Diag Protocol, Uncompressed Len: 1051

- Header
- Compression Header
- Message
 - Item: APPL, ST_R3INFO, SUPPORTDATA, Len=32
 - Item: APPL, ST_R3INFO, CODEPAGE_DIAG_GUI, Len=15, Codepage number (numeric representation)=4110, Mini
 - Item: APPL, ST_R3INFO, CODEPAGE_APP_SERVER_1, Len=32, Codepage number (numeric representation)=4103, M
 - Item: APPL, ST_R3INFO, CONTEXTID, Len=32, Value=5A34CCE187C1F1468E58000C297D2E11
 - Item: APPL, ST_R3INFO, DBNAME, Len=3, Value=NSP
 - Item: APPL, ST_R3INFO, CPUNAME, Len=13, Value=win2003-NW702
 - Item: APPL, ST_R3INFO, USERID, Len=2, User ID=16093
 - Item: APPL, ST_R3INFO, MODENUMBER, Len=2, Mode Number=0
 - Item: APPL, ST_R3INFO, IMODENUMBER, Len=2, IMode Number=0
 - Item: APPL, ST_R3INFO, IMODEUUIDS2, Len=18
 - Item: APPL, ST_R3INFO, GUI_THEME, Len=10, Value=TRADESHOW
 - Item: APPL, ST_R3INFO, KERNEL_VERSTON, Len=12, Database version=702, Kernel version=7200, Kernel patch

0000 10 06 11 00 20 ff 7f fe 2d d8 b7 37 d6 74 08 7e? ..7.t~
0010 13 05 97 15 97 eb f2 3f 8d 03 70 ff 0f 00 00 00? ..p.....

Frame (659 bytes) Uncompressed Data (1051 bytes)

Packet crafting

- Scapy classes
 - SAPNi
 - SAPDiagDP (DP Header)
 - SAPDiag (Diag header + compression)
 - SAPDiagItem
 - Custom classes for relevant Diag items
- PoC and example scripts
 - Information gathering
 - Login Brute Force
 - Proxy/MITM script
 - Diag server

Fuzzing approach

- Fuzzing scheme using
 - scapy classes
 - test cases generation
 - delivery
 - windbg
 - monitoring
 - xmlrpc
 - synchronization
- Monitoring of all work processes

Vulnerabilities found

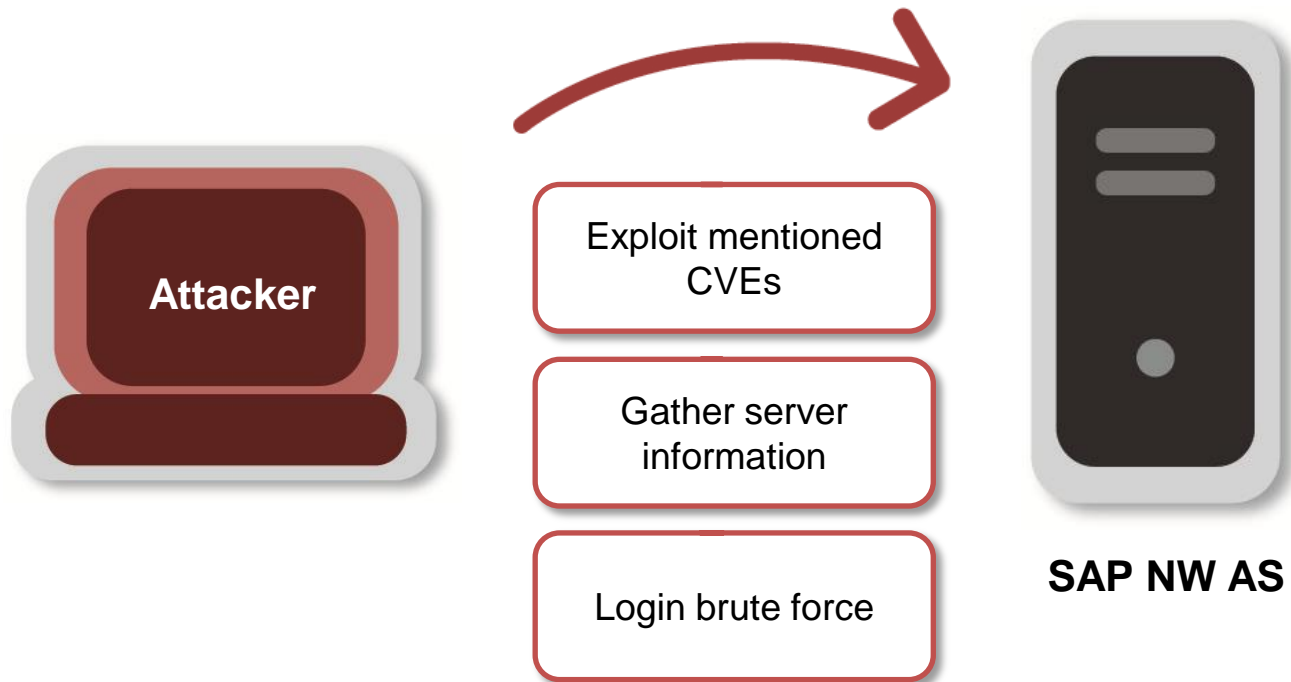
- 6 vulnerabilities released on May 2012 affecting SAP NW 7.01/7.02, fix available on SAP Note 168710
- Unauthenticated remote denial of service when developed traces enabled
 - CVE-2012-2511 – DiagTraceAtoms function
 - CVE-2012-2512 – DiagTraceStreamI function
 - CVE-2012-2612 – DiagTraceHex function

Vulnerabilities found

- Unauthenticated remote denial of service
 - CVE-2012-2513 – Diaginput function
 - CVE-2012-2514 – DiagiEventSource function
- Unauthenticated remote code execution when developer traces enabled
 - CVE-2012-2611 – DiagTraceR3Info function
 - Stack-based buffer overflow while parsing ST_R3INFO CODEPAGE item
 - Thanks to Francisco Falcon (@fdfalcon) for the exploit

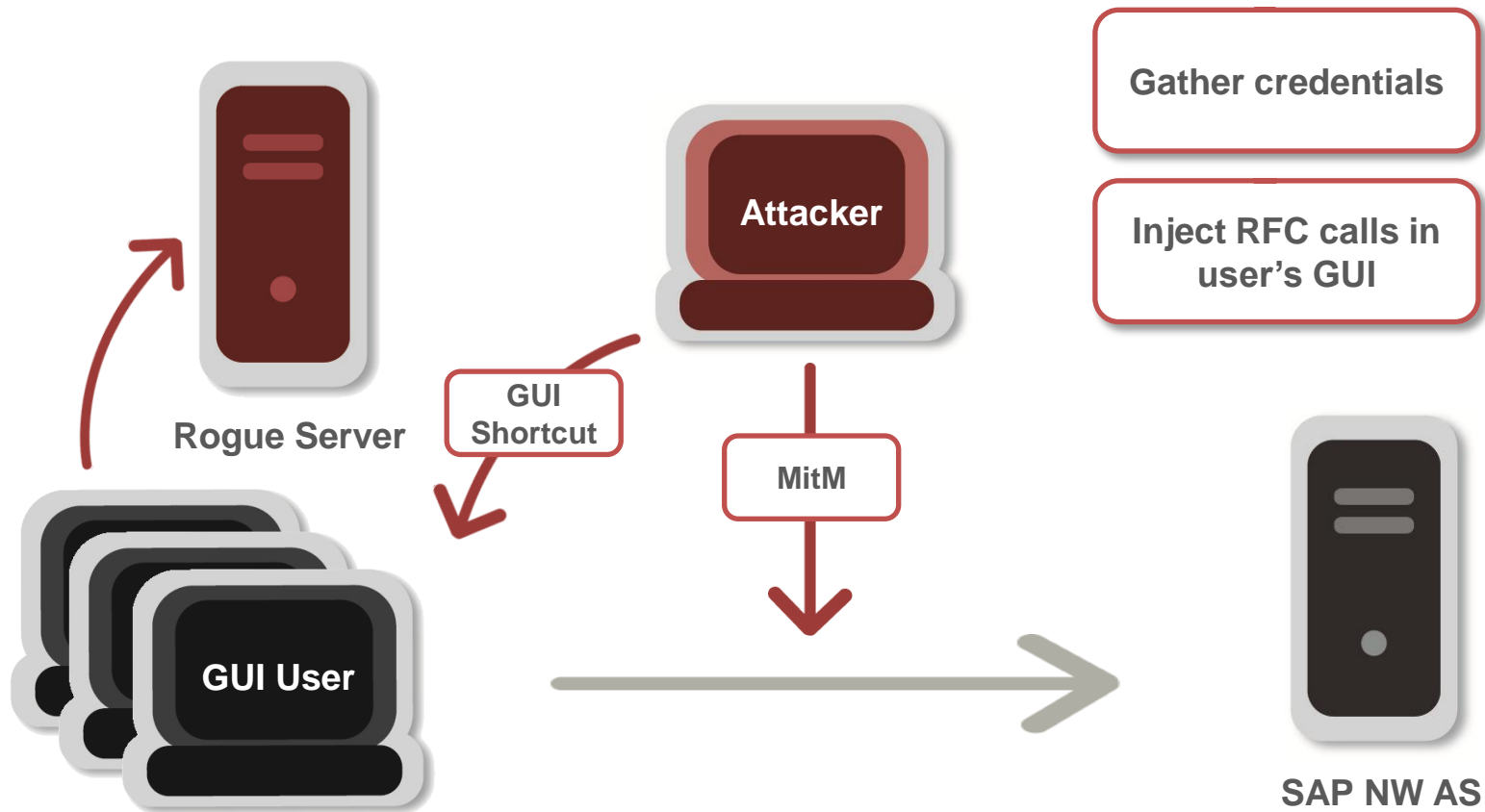
Attack scenarios

Target applications servers



Attack scenarios

Target GUI users



Agenda

- Introduction
- Motivation and related work
- SAP Netweaver architecture and protocols layout
- Dissecting and understanding the Diag protocol
- Results and findings
- Defenses and countermeasures
- Conclusion and future work

Defenses and countermeasures

Defenses and countermeasures

- Restrict network access to dispatcher service
 - TCP ports 3200-3298
 - Use application layer gateways
- Implement SNC client encryption
 - Provides authentication and encryption
 - Available for free at SAP Marketplace since 2011
 - See SAP Note 1643878
- Restrict use of GUI shortcuts
 - SAP GUI > 7.20 disabled by default
 - See SAP Note 1397000

Defenses and countermeasures

- Use WebGUI with HTTPS
 - See SAP Note 314568
- Patch regularly
 - Patch Tuesday
 - RSECNOTE program, see SAP Note 888889
- Patch CVEs affecting Diag
 - Look at CORE's advisory for mitigation/countermeasures
 - See SAP Note 168710
- Test regularly

Agenda

- Introduction
- Motivation and related work
- SAP Netweaver architecture and protocols layout
- Dissecting and understanding the Diag protocol
- Results and findings
- Defenses and countermeasures
- Conclusion and future work

Conclusion and future work

Conclusion

- Protocol details now available to the security community
- Practical tools for dissection and crafting of protocol's messages published
- New vectors for testing and assessing SAP environments
- Discussed countermeasures and defenses

Future work

- Security assessment and fuzzing of GUI/app server.
- Complete dissection of embedded RFC calls.
- Full implementation of attack scenarios
- Integration with external libraries and exploitation tools.
- Security assessment of SNC and coverage of encrypted traffic.

Q & A

Thank you !

**Thanks to
Diego, Flavio, Dana, Wata and Euge**

References

<https://service.sap.com/sap/support/notes/1643879>
http://www.secaron.de/Content/presse/fachartikel/sniffing_diag.pdf
<http://conus.info/RE-articles/sapgui.html>
http://www.sensepost.com/labs/conferences/2011/systems_application_proxy_pwnage
<http://ptresearch.blogspot.com/2011/10/sap-diag-decompress-plugin-for.html>
<http://www.oxid.it/index.html>
<https://service.sap.com/securitynotes>
http://help.sap.com/saphelp_nw70/helpdata/en/84/54953fc405330ee10000000a114084/frameset.htm
http://www.troopers.de/wp-content/uploads/2011/04/TR11_Wiegenstein_SAP_GUI_hacking.pdf
http://www.virtualforge.com/tl_files/Theme/Presentations/The%20ABAP%20Underverse%20-%20Slides.pdf
<http://www.wireshark.org/>
<http://www.secdev.org/projects/scapy/>
<http://www.coresecurity.com/content/sap-netweaver-dispatcher-multiple-vulnerabilities>
<https://service.sap.com/sap/support/notes/1687910>
http://help.sap.com/saphelp_nw70ehp2/helpdata/en/47/cc212b3fa5296fe10000000a42189b/frameset.htm
<https://service.sap.com/sap/support/notes/1643878>
<https://service.sap.com/sap/support/notes/1397000>
<https://service.sap.com/sap/support/notes/314568>
<https://service.sap.com/sap/support/notes/888889>