CentraleSupélec within

IRISA, UMR CNRS 6074

INSTITUT DE RECHERCHE EN INFORMATIQUE ET SYSTÈMES ALÉATOIRES

Research axes

Irisa, Research Institute in Computer Science and Random Systems, is currently the largest French research laboratory (850+ people) in the field of computer science and information technology. The laboratory covers all the themes within these fields, from computer and network architecture to artificial intelligence, including, e.g., software engineering, distributed systems and virtual reality.

IRISA, is a joint laboratory of nine institutions, in alphabetical order CentraleSupélec, the CNRS, ENS Rennes, IMT Atlantique, Inria, INSA Rennes, Inserm and Rennes and South Brittany universities. Focused on the future of computer science at large, with internationally recognized expertise, IRISA is present on three sites in Brittany (Rennes, Lannion, Vannes), at the heart of a rich regional research and innovation ecosystem.

Its multidisciplinary approach gives rise to a force of women and men who give their best for the fundamental and applied research, training, exchanges with other disciplines, scientific mediation, know-how and technology transfer.

In order to remain at the leading edge of computer science and information technology, while accompanying the digital transition of society and other scientific disciplines, the laboratory is structured in seven scientific departments, along with seven transversal axes addressing societal challenges such as cybersecurity, health, environment and ecology, transport, robotics, energy, and culture.

The Rennes campus of CentraleSupélec houses one of the 40 teams of the laboratory.

CIDRE TEAM (Confidentiality, Integrity, Disponibility & Repartition)

CIDRE is a joint research group between Inria, Rennes university, CNRS and CentraleSupélec, focusing on the security of distributed information systems. The long-term ambition of the team is to contribute to build distributed systems that are trustworthy and respectful of privacy, even when some nodes in the system have been compromised.

With this objective in mind, the CIDRE group focuses on three different aspects of security, namely trust, intrusion detection, and privacy as well as on the bridges that exist between these aspects.

With this objective in mind, the CIDRE team focuses mainly on the three following topics:

- Attack comprehension
- Attack detection
- Attack resistance.

HIGHLIGHTS 2023

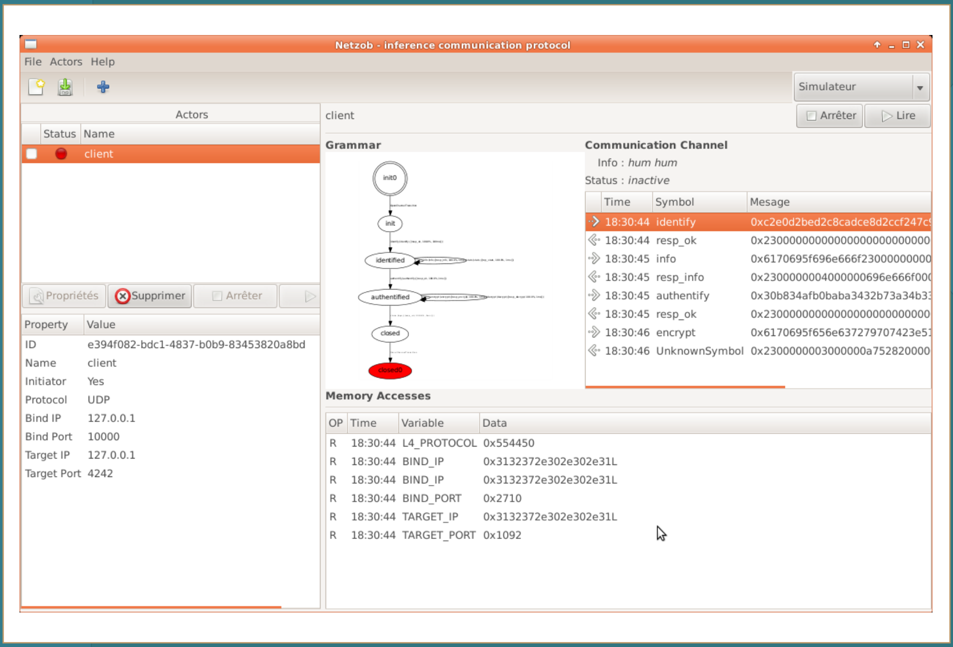
Accepted projects: **PEPR Defmal**, **SecureEval**

Accepted project: **CMA Cyber**

FRANCE 2030
PROGRAMME DE RECHERCHE
CYBERSÉCURITÉ

New organization proposal about CIDRE team to be splitted into two teams: **PIRAT** and **SUSHI** in 2024

EXAMPLES OF STUDIES



	Status	Name
□	●	client

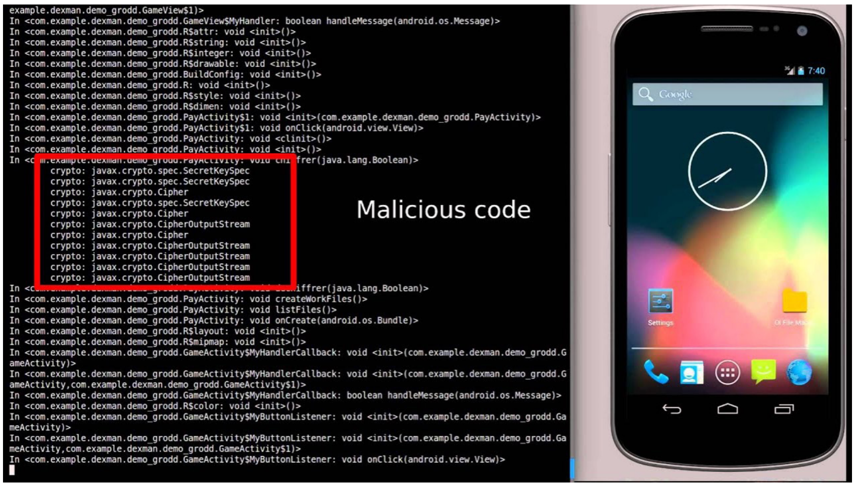
Property	Value
ID	e394f082-bdc1-4837-b0b9-83453820a8bd
Name	client
Initiator	Yes
Protocol	UDP
Bind IP	127.0.0.1
Bind Port	10000
Target IP	127.0.0.1
Target Port	4242

Info : *hum hum*
Status : *inactive*

Time	Symbol	Mesage
18:30:44	identify	0xc2e0d2bed2c8cadce8d2ccf247c
18:30:44	resp_ok	0x23000000000000000000000000
18:30:45	info	0x6170695f696e666f23000000000
18:30:45	resp_info	0x2300000000400000696e666f00
18:30:45	authentify	0x30b834afb0baba3432b73a34b3
18:30:45	resp_ok	0x23000000000000000000000000
18:30:46	encrypt	0x6170695f656e637279707423e5
18:30:46	UnknownSymbol	0x2300000003000000a752820000

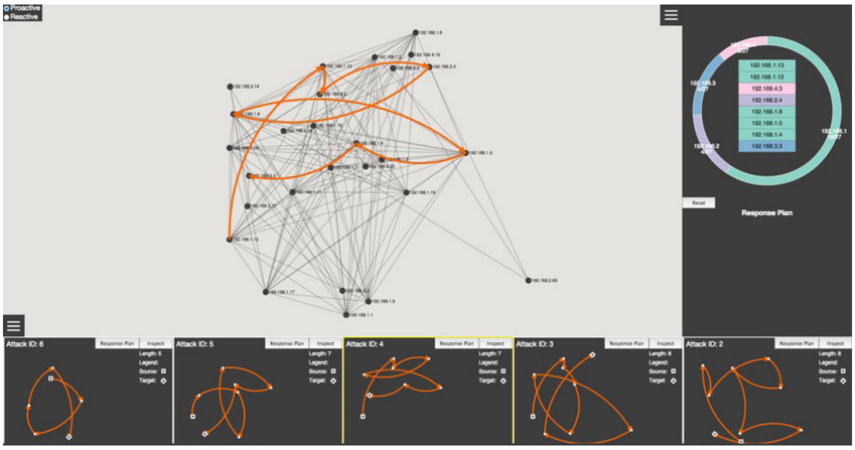
OP	Time	Variable	Data
R	18:30:44	L4_PROTOCOL	0x554450
R	18:30:44	BIND_IP	0x3132372e302e302e31L
R	18:30:44	BIND_IP	0x3132372e302e302e31L
R	18:30:44	BIND_PORT	0x2710
R	18:30:44	TARGET_IP	0x3132372e302e302e31L
R	18:30:44	TARGET_PORT	0x1092

Protocol Analysis with the Netzob software

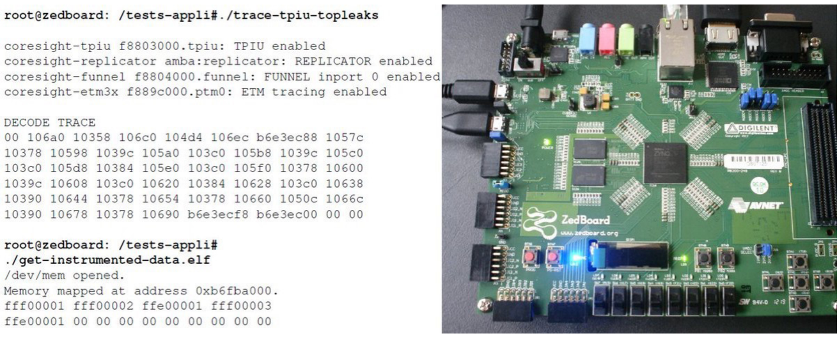


```
example.dexman.demo_grodd.GameView$1)>
In <com.example.dexman.demo_grodd.GameView$MyHandler: boolean handleMessage(android.os.Message)>
In <com.example.dexman.demo_grodd.R$attr: void <init>()>
In <com.example.dexman.demo_grodd.R$string: void <init>()>
In <com.example.dexman.demo_grodd.R$integer: void <init>()>
In <com.example.dexman.demo_grodd.R$drawable: void <init>()>
In <com.example.dexman.demo_grodd.BuildConfig: void <init>()>
In <com.example.dexman.demo_grodd.R: void <init>()>
In <com.example.dexman.demo_grodd.R$style: void <init>()>
In <com.example.dexman.demo_grodd.R$dimen: void <init>()>
In <com.example.dexman.demo_grodd.PayActivity$1: void <init>(com.example.dexman.demo_grodd.PayActivity)>
In <com.example.dexman.demo_grodd.PayActivity$1: void onClick(android.view.View)>
In <com.example.dexman.demo_grodd.PayActivity: void <clinit>()>
In <com.example.dexman.demo_grodd.PayActivity: void <init>()>
In <com.example.dexman.demo_grodd.PayActivity: void chiffrer(java.lang.Boolean)>
        crypto: javax.crypto.spec.SecretKeySpec
        crypto: javax.crypto.spec.SecretKeySpec
        crypto: javax.crypto.Cipher
        crypto: javax.crypto.spec.SecretKeySpec
        crypto: javax.crypto.Cipher
        crypto: javax.crypto.CipherOutputStream
        crypto: javax.crypto.Cipher
        crypto: javax.crypto.CipherOutputStream
        crypto: javax.crypto.CipherOutputStream
        crypto: javax.crypto.CipherOutputStream
        crypto: javax.crypto.CipherOutputStream
In <com.example.dexman.demo_grodd.PayActivity: void dechiffrer(java.lang.Boolean)>
In <com.example.dexman.demo_grodd.PayActivity: void createWorkFiles()>
In <com.example.dexman.demo_grodd.PayActivity: void listFiles()>
In <com.example.dexman.demo_grodd.PayActivity: void onCreate(android.os.Bundle)>
In <com.example.dexman.demo_grodd.R$layout: void <init>()>
In <com.example.dexman.demo_grodd.R$mipmap: void <init>()>
In <com.example.dexman.demo_grodd.GameActivity$MyHandlerCallback: void <init>(com.example.dexman.demo_grodd.G
ameActivity)>
In <com.example.dexman.demo_grodd.GameActivity$MyHandlerCallback: void <init>(com.example.dexman.demo_grodd.G
ameActivity,com.example.dexman.demo_grodd.GameActivity$1)>
In <com.example.dexman.demo_grodd.GameActivity$MyHandlerCallback: boolean handleMessage(android.os.Message)>
In <com.example.dexman.demo_grodd.R$color: void <init>()>
In <com.example.dexman.demo_grodd.GameActivity$MyButtonListener: void <init>(com.example.dexman.demo_grodd.Ga
meActivity)>
In <com.example.dexman.demo_grodd.GameActivity$MyButtonListener: void <init>(com.example.dexman.demo_grodd.Ga
meActivity,com.example.dexman.demo_grodd.GameActivity$1)>
In <com.example.dexman.demo_grodd.GameActivity$MyButtonListener: void onClick(android.view.View)>
```

Execution of Android malicious code with GroddDroid



VEGAS: security alerts visualization



```
root@zedboard: /tests-appli#./trace-tpiu-topleaks

coresight-tpiu f8803000.tpiu: TPIU enabled
coresight-replicator amba:replicator: REPLICATOR enabled
coresight-funnel f8804000.funnel: FUNNEL inport 0 enabled
coresight-etm3x f889c000.ptm0: ETM tracing enabled

DECODE TRACE
00 106a0 10358 106c0 104d4 106ec b6e3ec88 1057c
10378 10598 1039c 105a0 103c0 105b8 1039c 105c0
103c0 105d8 10384 105e0 103c0 105f0 10378 10600
1039c 10608 103c0 10620 10384 10628 103c0 10638
10390 10644 10378 10654 10378 10660 1050c 1066c
10390 10678 10378 10690 b6e3ecf8 b6e3ec00 00 00

root@zedboard: /tests-appli#
./get-instrumented-data.elf
/dev/mem opened.
Memory mapped at address 0xb6fba000.
fff00001 fff00002 ffe00001 fff00003
ffe00001 00 00 00 00 00 00 00 00 00
```

Hardware information flow monitoring with HardBlare

Industrial Partners

- CISCO,
- Hackuity,
- HEWLETT-PACKARD,
- Malizen,
- NOKIA,
- OBERTHUR,
- ORANGE,
- THALES...

Academic Partners

University of Luxembourg, ENSI Bourges, ENSI Caen, IMT, INSERM, LabSTICC, LAAS, La Sapienza University, LIRIS, Nantes University, National University of Singapore, Technische Universitat of Hamburg-Harburg

Key figures*

Professors, Associate Professors & Researchers	19
PhD Students	14
PostDoc	1
Visiting Professor	1
Publications of the year (WoS)	8

*CentraleSupélec only

www.rennes.centralesupelec.fr/recherche

Director of CentraleSupélec's Rennes campus: Yves LOUET

☎ +33 (0)2 99 84 45 34

✉ yves.louet@centralesupelec.fr

Head of CIDRE team: Valérie Viet Triem Tong

☎ +33 (0)2 99 84 45 73

✉ valerie.viettriemtong@centralesupelec.fr

Assistant: Myriam Andrieux

☎ +33 (0)2 99 84 45 50

✉ myriam.andrieux@centralesupelec.fr

CentraleSupélec
Rennes Campus
Avenue de la Boulaie
CS 47601
F-35576 Cesson-Sévigné Cedex

July 2024