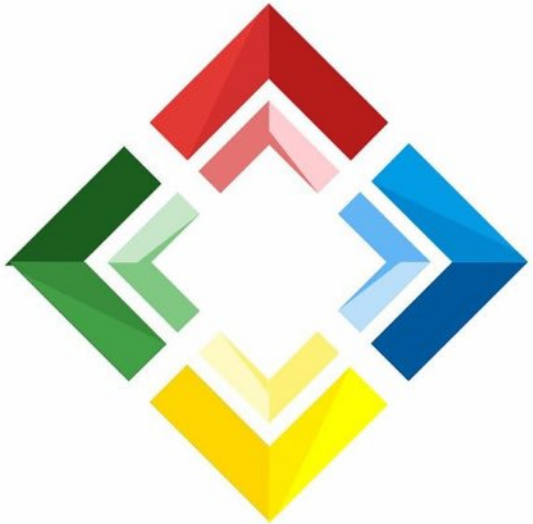
Dipartimento di Informatica,
Sistemistica e Comunicazione

Dipartimento di Giurisprudenza



Bicocca Security Lab

UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

What is BiS Lab

The BiS Lab (Bicocca Security lab) is a research laboratory of the Milan-Bicocca University dedicated to security in Information Technology. The BiS Lab, combining the skills of researchers of the Department of Computer Science and of the Department of Law, aims at responding to cyber security challenges, not only from a technological point of view but also from a legal point of view, designing software and policies that can be of simple use and effective.

UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

BiS Lab

The integrated approach of BiS Lab

Our University has an important goal alongside traditional ones of higher education and scientific research: dialogue with society, mainly through (but not limited to) technology transfer and public good creation.

BiS Lab embraces integration and interaction.

UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

BiS Lab

The impact of Security

The latest statistics show how computer security incidents involve not only big corporations, but also the everyday use of the network by common users.

Data provided in the last few years by Europol's European Cybercrime Center (EC3) show how the demand for online services and products has increased, and the number of criminals willing to meet them has increased: terrorism, drug trafficking, extortion, ransoms, money laundering, smuggling of counterfeit material or of pedopornographic material; There is no aspect of criminal life that has no derivation inside the network and this gives life, according to published studies, to an illicit business whose profits amount to 750 billion euros a year.

Who is in BiS Lab?

BiS Lab was born as a research group linking different disciplines, mainly Computer Science and Law.

Now it gathers for its activities around fifteen people: faculty, students, professionals.

Principal investigators are (CVs in last slides):

Claudio Ferretti and Alberto Leporati (Dip.Informatica, Sist. e Com.),

Andrea Rossetti (Dip. Giurisprudenza).

UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

BiS Lab

Activities of BiS Lab

BiS Lab is developing:

-technological research

-education and training

-dissemination of culture and knowledge of security

-legal and technological assistance to industry

UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

BiS Lab

Activities: Research

Technological research in BiS Lab has the primary goal of facilitating the safe use of computer tools by users and operators. Research activities are centered on a variety of technologies that help dominate the complexity in ICT of data and applications (examples follows).

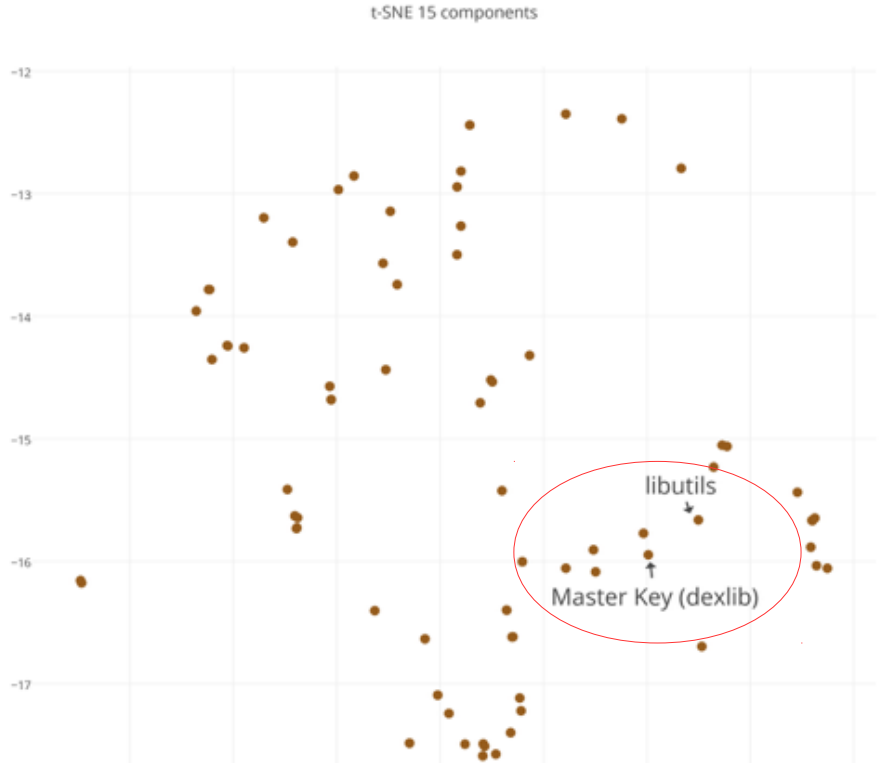
UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

BiS Lab

Research: machine learning & secure code

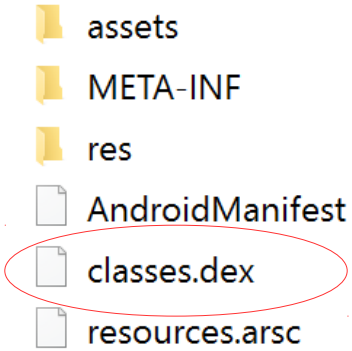
Using machine learning to find vulnerabilities in source code:

```
Functions in cluster 41
----
build/tools/zipalign/ZipFile.cpp_59:0_130:0_ZipFile :: open
build/tools/zipalign/ZipFile.cpp_646:0_669:0_ZipFile :: copyFpToFp
build/tools/zipalign/ZipFile.cpp_701:0_735:0_ZipFile :: copyPartialFpToFp
build/tools/zipalign/ZipFile.cpp_897:0_942:0_ZipFile :: flush
build/libs/host/CopyFile.c_116:0_151:0_copyFileContents
bootable/recovery/recovery.c_225:0_247:0_copy_log_file
bootable/recovery/edify/expr.c_102:0_124:0_IfElseFn
bootable/recovery/edify/expr.c_126:0_138:0_AbortFn
bootable/recovery/edify/expr.c_175:0_186:0_StdoutFn
bootable/recovery/edify/expr.c_188:0_198:0_LogicalAndFn
bootable/recovery/edify/expr.c_200:0_210:0_LogicalOrFn
bootable/recovery/edify/expr.c_212:0_219:0_LogicalNotFn
bootable/recovery/edify/expr.c_221:0_235:0_SubstringFn
bootable/recovery/edify/expr.c_237:0_250:0_EqualityFn
bootable/recovery/edify/expr.c_252:0_265:0_InequalityFn
bootable/recovery/updater/install.c_296:0_314:0_ShowProgressFn
bootable/recovery/updater/install.c_316:0_331:0_SetProgressFn
bootable/recovery/updater/install.c_334:0_354:0_PackageExtractDirFn
bootable/recovery/updater/install.c_662:0_675:0_GetPropFn
bootable/recovery/updater/install.c_876:0_893:0_ApplyPatchSpaceFn
bootable/recovery/updater/install.c_969:0_993:0_ApplyPatchCheckFn
frameworks/base/libs/utils/ZipFileRO.cpp_323:0_380:0_ZipFileRO ::
parseZipArchive
frameworks/base/libs/utils/ZipFileRO.cpp_672:0_726:0_ZipFileRO ::
uncompressEntry
frameworks/base/libs/utils/BackupHelpers.cpp_853:0_898:0_compare_file
frameworks/base/libs/utils/String16.cpp_257:0_291:0_String16 :: insert
frameworks/base/libs/utils/Asset.cpp_436:0_497:0__FileAsset :: read
frameworks/base/libs/utils/ZipUtils.cpp_268:11_343:0_ZipUtils :: examineGzip
dalvik/dexdump/DexDump.cpp_1288:0_1340:0_dumpSField
dalvik/dexdump/DexDump.cpp_1581:0_1640:0_dumpMethodMap
dalvik/tools/dmtracedump/TraceDump.c_2624:0_2802:0_createDiff
dalvik/tools/dmtracedump/CreateTestTrace.c_378:0_414:0_writeKeyMethods
dalvik/libdex/DexSwapVerify.cpp_1601:0_1643:0_crossVerifyClassDataItem
```



Research: looking for malware in Android

Decomposing Android apps to automatically classify them (with machine learning):




```
.method protected onCreate(Landroid/os/Bundle;)V
    .locals 3
    .parameter "savedInstanceState"
    .prologue
    invoke-super {p0, p1}, Landroid/app/Activity
     ;->onCreate(Landroid/os/Bundle;)V

     const/high16 v0, 0x7f03

const-string v0, "StartActivity:"
const-string v1, “Message"
 invoke-static {v0, v1}, Landroid/util/Log;
       ->d(Ljava/lang/String;Ljava/lang/String;)I
 move-result v0

    return-void
.end method
```

Smali Byte code

UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

BiS Lab

Activities: Education and Training

The goal of enhancing security is also pursued by seeking to increase the perception of dangers and the adoption of best practices in the use of ICT, with good dissemination, but also developing user interfaces that guide users to the construction of correct mental models of how the tools work.

Accordingly, BiS Lab offers intensive courses (a few days long) for industrial and governative operators, or for researchers from outside the computer security field.

UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

BiS Lab

Other Activities:

Dissemination of culture and knowledge of security:

BiS Lab regulary offers public meetings and seminars on security topics, and actively participates in onine discussions and focused social networks

Legal and technological assistance to industry:

BiS Lab can assist businesses willing to assess their technological security status, or their compliance to requirements of regulatory institutions (e.g. European General Data Protection Regulation in 2018)

UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

BiS Lab

Claudio Ferretti

Claudio Ferretti teaches Computer Security (for Master's Degree).

PhD, post-doc in Japan (STS-JSPS 1995-1996). He has published 40 articles (bio-inspired computational models, security) in international scientific journals and in international workshops and conference proceedings (all with peer-review), and 1 book chapter (Oxford University Press). He has been active in several nationally-funded research projects (including local director of research for PRIN 2004), international projects (TOISE), and technology transfer activities (contracts between university and companies).

UNIVERSITA' DEGLI STUDI DI MILANO BICOCCA

BiS Lab

Alberto Leporati

Alberto Leporati teaches Programming and Information Theory.

PhD, he has published 40 articles (computing, complexity, encryption) in international scientific journals, 3 book chapters, and 41 articles in international workshops and conferences (all with peer-review). He has been part of several nationally-funded research projects (MIUR / COFIN 2001, MAP / FIT 2002, PRIN 2004, PRIN 2007), international projects (SMART, TOISE) and activities of technology transfer (contracts between university and companies).

UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

BiS Lab

Andrea Rossetti

Andrea Rossetti teaches Philosophy of Law and Legal Informatics. Since 1999, he has been involved in Legal Informatics; in particular he has authored some essays focused on the idea of "openness" in ICT; he was editor of the manual: “Legal Informatics”.

From 2002 to 2008 he directed the new law course of “Law and new technologies” at the State University of Milan and later at the University of Milano-Bicocca.

He was the leader of the Legal Team for the European Illbuster Project (2012-2014):

http://illbuster-project.eu/

UNIVERSITA' DEGLI STUDI DI MILANO BICOCCA

BiS Lab

Some previous international projects (1/3)

ILLBUSTER

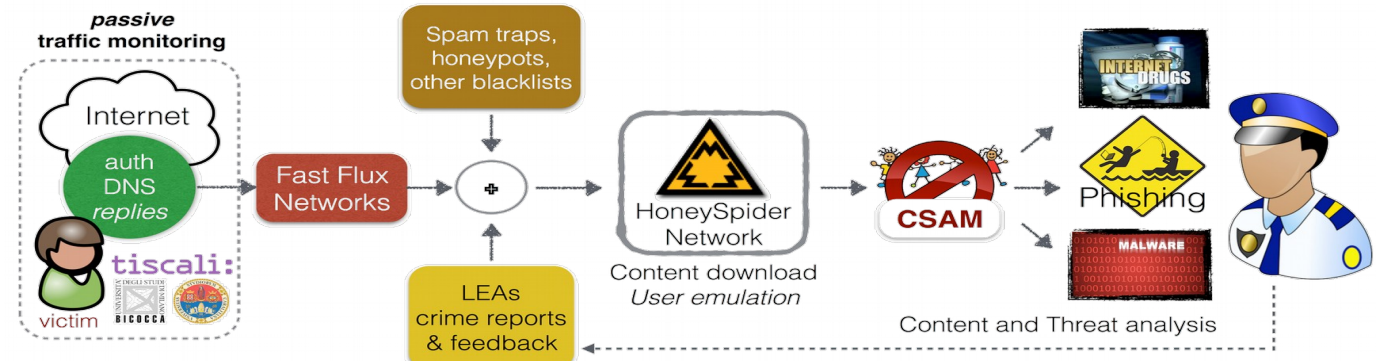
HOME | PROJECT | PARTNERS | EVENTS | PUBLICATIONS | MEDIA | DOWNLOADS

Buster of ILLegal contents spread by malicious computer networks

With the financial support of the **Prevention of and Fight against Crime** Programme.
European Commission - Directorate General Home Affairs

ILLBuster is a project funded by the **European Commission** (DG-HOME) within the programme "Prevention of and Fight against Crime". The goal of the project is to develop an integrated information system for the semi-automatic discovery of illegal activities over the Internet. The system is aimed to be a valuable tool to be used by LEAs for their activities of prevention of and fight against cyber-crime.

Fast-Flux Threat Map now available!
Developed by **PRA Lab** for the ILLBuster project



UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

BiS Lab

Some previous international projects (2/3)

The SMART project

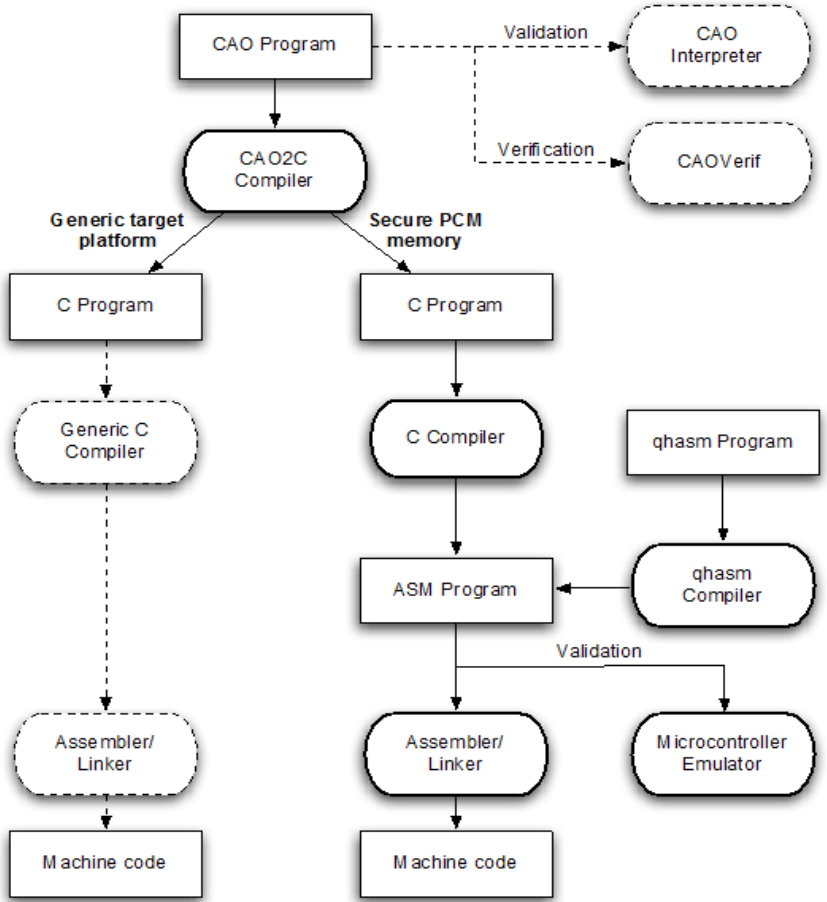
Project Acronym: SMART
Project full title: Secure Memories and Applications Related Technologies

Grant Agreement Number: 120224

Duration of Project: 01 January 2010 – 31 August 2013

Project Coordinator: Maurizio Gaibotti, Micron Semiconductor Italia

THALES MULTICERT gemalto teletel Micron cnes ISD S.A. Integrated Systems Development Universidade do Minho ARISTOTLE UNIVERSITY OF THESSALONIKI UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA



Some previous international projects (3/3)

CALL 2010

eniac JOINT UNDERTAKING

Project profile

TOISE

Trusted computing for European embedded systems

In the future, critical applications such as smart grids for electricity networks, smart metering, environmental or infrastructure sensor networks and the management of trusted components will require development and implementation of secure technologies to provide smarter and safer operation. Trusted computing systems used in personal computers and workstations offer a proven security mechanism and could be adaptable for this purpose. The ENIAC JU project TOISE aims to develop such tamper-resistant solutions for embedded applications and boost European leadership in secure integrated devices.

UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

BiS Lab