Work at the leading edge of media and entertainment technology. Join the 300 Technicolor researchers and engineers who are breaking new ground in digital innovation and inventing the future of digital media to create outstanding content and deliver unique consumer experiences for the home, theaters and on-the-go. In any of Technicolor Laboratories, you will discover a group of talented individuals from diverse backgrounds working together in a stimulating, state-of-the-art environment that fosters new ideas and unleashes creativity.

Security and Content Protection – Summer Internships 2014

Security and Content Protection is one of the Technology Areas hosted by Technicolor's Content Platform and Security Lab located in Rennes (France), which is the largest research centre of the group. It is composed of security experts whose objectives are to deter piracy on high-value content from creation to consumption and to secure the digital home (gateways, set-top boxes, tablets). Their activities are organized along three main lines:

1. Conduct innovative research in cryptography, multimedia security, secure platforms, software obfuscation, etc;
2. Transfer security components to sustain Technicolor's product line e.g. ContentArmor™;
3. Provide counsel and guidance to Technicolor's Business Units to help them designing secure products and services.

TOPICS

Depending on the profile of the applicant, the internship will focus either on research or development. Topics of interest include (but are not limited to):

- Efficient and secure implementations of cryptographic algorithms;
- Network and cloud security;
- Multi-platforms software security;
- Prototyping of new security features for Technicolor products;
- Signal processing for multimedia security: watermarking, fingerprinting, passive forensics tools, etc.

Technicolor has a strong intellectual property strategy and results will be patented when possible. The results of the internship may also be disseminated by publishing articles in scientific conferences and publications. For more applied topics, the internship could yield a demo, a prototype, or even an integration in Technicolor products.

PROFILE

- M.Sc. student and/or 3rd year of engineering school
- Inquiring mind, inventive, passionate about security and/or signal processing
- One or more of the following skills: cryptography, hacking techniques, network security, signal processing and analysis
- Skills in prototyping applications on PC or embedded platforms
- Good writing and oral communications skills
- Fluent in English

Company / Group: Technicolor (www.technicolor.com) / Research & Innovation (www.technicolor.com/en/innovation)
Position: 6-months intern
Location: Rennes, FRANCE (http://research.technicolor.com/rennes)

If you are interested in joining us, please visit our website and consult our internship open positions at
http://research.technicolor.com/rennes/job-opportunities

technicolor
www.technicolor.com

technicolor

Technicolor R&D France Snc
975 av des Champs Blancs – CS 17616
35576 Cesson-Sévigné Cedex - France

tél. + 33 (0)2 99 27 30 00
fax + 33 (0)2 99 27 30 01

Internship proposal for 2014
Proposal ref: PSL_SCP_001

Title of internship: Signal Processing for Multimedia Security

Internship period & duration: 6 months e.g. March-August 2014 (can be adjusted)

Working environment: The selected candidate will join a team of 6 researchers and engineers working on signal processing for multimedia security. The members of the team are located in Rennes (France) in the new facilities of Technicolor R&D France, the largest Research Centre of the group.

Context: The rapid transition from analog to digital media over the last decades put the Entertainment industry under increased pressure to protect their high-valued assets. Piracy has indeed been significantly facilitated with the commercial deployment of software to manipulate digital content, and the development of rapid and efficient distribution networks. To tackle this issue, content protection mostly relies on (i) cryptography to prevent unauthorized access to assets, (ii) jamming to interfere with illegal recording, (iii) content fingerprinting to identify assets collected over the Internet, (iv) digital watermarking to provide a tracing mechanism to be able to pinpoint the source of a leak when it occurs, and (v) passive forensics techniques to characterize pirate samples.

Objective: The intern will contribute to Technicolor's effort to propose innovative solutions in content protection. Depending on the profile of the applicant, the internship will focus either on research or development. Topics of interest include (but are not limited to):

HEVC watermarking. Technicolor's video watermarking technology is currently tied to the H.264/AVC video codec by design. The intern will investigate how to export our 2-step watermarking strategy to the HEVC coding format and will modify a reference decoder to implement a first version to enlarge the scope of Technicolor's offer.

Watermarking stereo video. Stereo content raises unique challenges for digital watermarking, both in terms of robustness and fidelity. State-of-the-art techniques started to account for the depth information but still do not properly accommodate for inconsistent disparity estimation, e.g. left→right vs. right→left. The embedding rate of proposed techniques also remains limited. The intern will investigate novel strategies to tackle these limitations.

3D mesh watermarking. The increasing popularity of 3D models calls for dedicated mesh watermarking. Robustness to non connectivity preserving attacks, such as pose or cropping, still remains an open issue today. To tackle this challenge, the intern will define a robust canonical partitioning method and integrate it in a state-of-the-art 3D watermarking system.

Fidelity models. Digital watermarks inserted into multimedia content should be unnoticeable to the average viewer. To guarantee such imperceptibility, it is common practice to rely on perceptual models. However, conventional models are tailored for compression and may not be readily usable in watermarking. Depending on the her profile and interest, the intern will study how to measure perceived distortion when only a few blocks are modified in a video or when noise is added to stereo video content.

Video re-alignment. Relying on content-dependent salient features such as key-frames is necessary to realign a pirate video with its corresponding master. For accuracy, the extraction, localization and matching of these key frames should be robust to severe degradation. The intern will explore alternate key frames extraction strategies as well as new temporal consistency constraints to improve the accuracy of Technicolor's resynchronization framework.

Piracy path. Screencasting, aka. recording what is displayed on a PC screen, is on the verge of replacing camcording as a piracy threat. Both video watermarking and fingerprinting are expected to be robust against display-and-record pipeline, but is hardly validated in practice due to the required tedious benchmarking campaigns The intern will analyze all the mechanisms occurring along the piracy path to (i) model the distortions experienced by the content and/or (ii) design an efficient mimicry piracy simulator.

Passive video forensics. Forensic analysis may significantly differ depending on the genesis of the pirate copy (camcording, screencasting, HDMI strip, DVD/BD rip). Sample classification by visual inspection is error prone and time consuming. To automate this task, the intern will develop such a classifier, based on conventional classification techniques (e.g. SVM) trained with video features discriminating between the types of piracy.

Candidates, who have a general interest in multimedia security but do not find an appealing internship in the list above, are encouraged to contact M. Bertrand Chupeau directly by email (bertrand.chupeau@technicolor.com) to discuss potential internship topics and assess whether they are in line with Technicolor's strategy.

Profile of the applicant: 3rd year engineer or master, specialized in signal processing.

Prerequisites:

- Signal processing fundamentals e.g. filtering, denoising, estimation, segmentation, indexing, compression, etc;
- Multimedia security e.g. DRM, watermarking, fingerprinting, forensics, biometrics, steganography;
- [opt.] Machine learning, statistics, optics, communications, human perception;
- Linux/windows environment;
- C/C++ programming, Matlab;
- Fluent English.

Apply at: stage.rennes@technicolor.com

technicolor

Technicolor R&D France Snc
975 av des Champs Blancs – CS 17616
35576 Cesson-Sévigné Cedex - France

tél. + 33 (0)2 99 27 30 00
fax + 33 (0)2 99 27 30 01

Internship proposal for 2014
Proposal ref : PSL_SCP_002

Title of internship : Control Flow Graph based attacks

Summary of the internship (requested for R&I : 5-6 lines max in English + illustration 300*300)

Modern reverse-engineering techniques allow attackers to understand underlying algorithms structure of the software. A common method consists in studying its control flow graph (CFG) that statically shows all possible paths of executed instructions. To counter this kind of attack, encryption protection is not always possible and often not sufficient, so there is a need to evaluate alternative solutions. A known technique to make reverse engineering more complex consists in flattening its Control Flow Graph*. The goal of the internship is to analyse some implementations of this technique.

* Wang, C., Davidson, J., Hill, J., & Knight, J. (2001, July). Protection of software-based survivability mechanisms. In *Dependable Systems and Networks, 2001.*

Context

Modern reverse-engineering techniques allow attackers to understand underlying algorithms structure of the software. A common method consists in studying its control flow graph (CFG) that statically shows all possible paths of executed instructions. To counter this kind of attack, encryption protection is not always possible and often not sufficient, so we need to evaluate alternative solutions. A known technique to make reverse engineering more complex consists in flattening its Control Flow Graph*.

The efficiency of the CFG flattening is very dependent on its implementation. Technicolor would like to study different implementations and needs some new reversing tools to evaluate them.

* Wang, C., Davidson, J., Hill, J., & Knight, J. (2001, July). Protection of software-based survivability mechanisms. In *Dependable Systems and Networks, 2001.*

Objective

The goal of this internship is to design and develop some tools to reverse binaries protected with CFG flattening. This should allow us to evaluate and improve some CFG flattening implementation.

Task description

The student will study the state of the art in CFG flattening and in reversing techniques.
Following this study, he will design innovating methods and tools for attacking protected binaries. These tools should reconstruct a readable CFG and evaluate its level of protection using information collected during the execution of the application.

Keywords

Disassembly, reverse, security, software protection, software obfuscation, hacking, decompilation

Working environment : Security & Content Protection Labs in Cesson Sévigné, Rennes, France

Profile of the applicant / Prerequisites

Multiplatform environment (Android or IOS ARM binaries, X86)
Skilled in reverse engineering/ debugging at instruction level.
Experience in at least one assembly language would be an advantage.

Internship period & duration: Six months beginning between February and April 2014

technicolor

Technicolor R&D France Snc
975 av des Champs Blancs – CS 17616
35576 Cesson-Sévigné Cedex - France

tél. + 33 (0)2 99 27 30 00
fax + 33 (0)2 99 27 30 01

Proposition de stage de fin d'études – Année 2014
Ref Proposition : PSL_SCP_003

Intitulé du stage

Analyse de sécurité d'un service web permettant la protection de contenu vidéo puis étude et réalisation d'une application utilisant ce service Web à distance de façon sécurisée.

Résumé du sujet (demandé pour R&I : 5-6 lignes max en anglais + photo 300*300)

The goal of this internship is the security analysis of a service web that allows protecting video content, and the study and implementation of a secure application that remotely accesses this web service. The work will be done in the context of the ContentArmor™ project, a video content protection solution proposed by Technicolor.
The internship will be held in Cesson-Sevigné (near Rennes, France) in the « Content Platforms & Security / Security & Content Protection » laboratory.

Sujet détaillé

Contexte

Les contenus vidéos qui circulent lors des travaux de postproduction ont une forte valeur et doivent absolument être protégés. La solution Technicolor ContentArmor™ fournit une solution de protection de contenus. Une application Windows permet de protéger de tels contenus avant que ceux-ci ne soient distribués.
Il existe également une version « service web » de cette solution qui permet à un ou plusieurs postes distants d'effectuer les opérations de protection. Il faut alors proposer à l'utilisateur distant une interface (application ou page web) pour accéder aux services de protections et s'assurer que cet accès au service web ne compromet pas la sécurité du système de protection.

But

Le but du stage est l'analyse de sécurité d'un service web permettant la protection de contenu vidéo puis étude et la réalisation d'une application utilisant ce service web à distance de façon sécurisée.

Description des travaux

Le stagiaire devra effectuer une analyse de sécurité d'une implémentation existante utilisant une application ne faisant appel qu'à quelques-unes des fonctionnalités offertes par le service web. Il s'agira d'identifier les vulnérabilités potentielles et d'implémenter quelques scénarios d'attaques pouvant compromettre la sécurité des données circulant sur le réseau ou mettre en danger le serveur hébergeant le service web.
Au terme de cette analyse, le stagiaire proposera et implémentera des améliorations du service web et réalisera une interface cliente (application ou page web) qui permettra de solliciter le service web de façon sécurisée, notamment en mode multi clients.

Mots clés

Service web, réseaux, sécurité (authentification, autorisation…), interface utilisateur

Environnement de travail

Le stagiaire sera intégré au Laboratoire « Content Platforms & Security / Security & Content Protection » de Technicolor composé de 16 ingénieurs et chercheurs.
Le stage est basé à Cesson-Sévigné.

Profil du stagiaire / Compétences requises

Sécurité réseau
Service Web (http, REST, JSON).
Développeur (C#, html, C/C++, javascript/php)
Environnement Windows (visual studio, IIS)

Durée et période du stage

6 mois, début du stage entre février er avril 2014.

technicolor

Technicolor R&D France Snc
975 av des Champs Blancs – CS 17616
35576 Cesson-Sévigné Cedex - France

tél. + 33 (0)2 99 27 30 00
fax + 33 (0)2 99 27 30 01

Proposition de stage de fin d'études – Année 2014
Ref Proposition : PSL_SCP_004

Intitulé du stage

« Techniques d'obfuscation pour les algorithmes de chiffrement à clé publique »

Résumé du sujet

The goal of the internship is to study obfuscation techniques and propose new ones to protect against extraction of cryptographic keys from data memory. On an open platform like a PC, any software that performs cryptographic operations must, at some point, have the instructions and the key material loaded into the memory. A user can easily access that memory and then the key material. Obfuscation consists in hiding sensitive data, storing it in a modified representation in the code. Sensitive data are then recomputed during execution using a layer of complex code. Obfuscation forces an attacker to use reverse-engineering to locate and extract the keys from a memory dump.

Sujet détaillé

Contexte

Dans de nombreux cas d'utilisation, les systèmes de protection sont sujets à des attaques sur les machines hôtes sur lesquels les services de protection sont assurés. C'est le cas sur un PC par exemple, où les clés secrètes peuvent être facilement accessibles lorsque celles-ci transitent dans la mémoire vive. La protection des clés est un aspect essentiel de la sécurité de ces systèmes. Différentes techniques d'obfuscation ont été développées dans la littérature. Elles apportent une solution pratique et permettent d'atteindre, dans certains cas, un niveau de sécurité acceptable.

But

Le but du stage est l'implémentation obfusquée d'un algorithme à clé publique ainsi qu'une analyse de la robustesse de ces implémentations. Concernant les algorithmes de chiffrement, l'étudiant étudiera les crypto-systèmes tels que RSA ou ElGamal. Pour la signature numérique, il s'intéressera aux systèmes DSA et ECDSA.

Description des travaux

Le stage consiste à identifier un ou plusieurs algorithmes et d'étudier différentes techniques d'obfuscation ainsi que leurs performances. Cela impliquera notamment le choix de l'algorithme de chiffrement, du corps sous-jacent et de sa représentation, de l'arithmétique, ainsi que des techniques de masquage choisies.

Mots clés

Cryptographie, obfuscation, DPA, side-channel attacks.

Environnement de travail

Le stagiaire sera intégré à la cellule « Secure Design » du Laboratoire « Content Platforms & Security / Security & Content Protection » de Technicolor composé de 12 ingénieurs et chercheurs.
Le stage est basé à Cesson-Sévigné.

Profil du stagiaire / Compétences requises

Cryptographie, programmation en C, anglais technique

Durée et période du stage

6 mois, début du stage entre février er avril 2014.