UNIVERSITÀ DEGLI STUDI
DI TRENTO
Facoltà di Scienze MM.FF.NN.
Dipartimento di Matematica

TERZO WORKSHOP DI CRITTOGRAFIA "BUNNYTN" 2012

Lunedì 12 marzo 2012
Dipartimento di Economia, Università di Trento

Titoli ed abstract del Workshop di Crittografia "BunnyTN" – 12 marzo 2012

9:30-9:40 **Presentazione del workshop**
Prof. Massimiliano Sala, *Università di Trento*

9:40-10:05 **LFSR e complessità: un breve excursus**
Prof. Michele Elia, *Politecnico di Torino*

10:05 - 10:20 **Quantum key distribution: how to distill unconditionally secure keys**
Dott. Matteo Canale, *Università di Padova*

10:20 - 10:35 **A survey on block ciphers**
Dott. Anna Rimoldi, *Università di Trento*

10:35 - 10:55 *Coffee break*

10:55 - 11:20 **Vulnerabilità dei protocolli SSL/TLS**
Prof. Andrea Visconti, *Università di Milano*

11:20 - 11:35 **Enforcing Security Policies in Outsourced Environments**
Dott. Asghar Rizwan, *Università di Trento*

11:35 - 11:50 **OpenNET: un cluster altamente scalabile per la gestione di sistemi remoti e costruito con hardware di recupero**
Dott. Lorenzo Nicolodi, *Università di Bolzano*

11:50 - 12:05 **A computational forensic methodology for malicious application detection on Android OS**
Dott. Svetlana Voronkova, *Università di Bolzano*

12:05 - 12:20 **Tecnica di oscuramento del segnale radio con chiave crittografica basata su coordinate spaziali**
Dott. Mario Marcovecchio, *Università di Firenze*

12:20 - 12:35 **Automated Security Analysis of Cryptographic Protocols**
Dott. Alessandro Armando, *Fondazione Bruno Kessler*

12:35 - 13:00 **Unobservable intrusion detection based on call traces in paravirtualized systems**
Prof. Marino Miculan, *Università di Udine*

13:00 - 14:30 *Pranzo sociale*

14:30 - 15:30 **Premiazioni CryptoWars**

15:30 - 15:40 *Coffee break*

15:40 - 16:05 **Haruspex: analisi del rischio ICT con metodo Monte Carlo**
Dott. Claudio Telmon, *Università di Pisa*

16:05 - 16:20 **A new bound on the size of linear codes**
Dott. Emanuele Bellini, *Università di Trento*

16:20 - 16:35 **Risultati sulla decodifica dei codici da varietà affine**
Dott. Chiara Marcolla, *Università di Trento*

16:35 - 16:50 **Curve massimali definite su campi finiti di ordine piccolo**
Dott. Irene Platoni, *Università di Trento*

16:50 - 17:05 **Codici AG generalizzati da curve massimali**
Dott. Marco Calderini , *Università di Trento*

17:05 - 17:15 *Coffee break*

17:15 - 17:30 **Geometria dei two-point codes su curva Hermitiana**
Dott. Alberto Ravagnani, *Università di Trento*

17:30 - 17:45 **Ricerca di codici estremali autoduali di lunghezza 72**
Dott. Martino Borello, *Università di Milano-Bicocca*

LFSR e Complessità: un breve excursus

Prof. Michele Elia, Politecnico di Torino

9:40 - 10:05

La generazione di sequenze di simboli, che abbiano caratteristiche simili a quelle di sequenze genuinamente casuali, ossia constituite di simboli casuali, equiprobabili e statisticamente indipendenti, è di grande importanza sia in crittografia, sia in sistemi di modulazione numerica. Le sequenze prodotte dai registri lineari a scorrimento, comunemente detti LFSR (Linear Feedback Shift Register), tipicamente si presentano con caratteristiche simili alle sequenze genuinamente casuali, tuttavia mostrano, soprattutto per applicaioni crittografiche, debolezzze che debbono essere opportunamente compensate. Data, la predominante importanza delle sequenze binarie, in questa presentazione considereremo solo LFSR su $\mathbb{F}_2$. I LFSR sono macchine a stati finiti il cui stato $\mathbf{x}(n)$ al passo n è un vettore su $\mathbb{F}_2$ di dimensione k. Il cambiamento di stato è ottenuto operando su $\mathbf{x}(n)$ con una matrice non singolare $\mathbf{M}$, di tipo $k \times k$, i cui elementi sono elementi di $\mathbb{F}_2$: una sequenza $x_h(1), x_h(2), \ldots, x_h(n), \ldots$ prodotta considerando una qualsiasi componente $x_h(n)$ di $\mathbf{x}(n)$, si dice sequenza generata dal LFSR. Queste sequenze sono periodiche, ed il loro periodo dipende dal polinomio caratteristico $p(z)$ di $\mathbf{M}$, ed in subordine dal vettore iniziale $\mathbf{x}(0)$, pertanto matrici equivalenti generano sequenze aventi lo stesso periodo. Di particolare importanza sono le k-squenze, ossia le sequenze di periodo massimo data la lungheza k del LFSR. Peraltro, un blocco di simboli costituito dal periodo si può interpretare come parola di un codice ciclico. Per questa via si possono studiare molte proprietà delle sequenze, in particolare delle k-sequenze, sia di carattere combinatorio, sia di carattere statistico. La connessione di generiche sequenze binarie con sequenze generate da LFSR consente di definire il cosiddetto profilo di complessità lineare di una sequenza, concetto di notevole importanza nelle applicaioni crittografiche.

La classica struttura di registro a scorrimento fu, quasi sicuramente, adottata per ridurre la complessità tecnologica dei circuiti elettronici. In pratica per minimizzare il numero di addizioni binarie della trasformazione lineare definita da $\mathbf{M}$. Tre strutture sono le più utilizzate e saranno brevemente riviste:

i) la struttura nota come Fibonacci LFSR corrispondente alla matrice compagna di $p(z)$;

ii) la struttura nota come Galois LFSR corrispondente alla trasposta della matrice compagna di $p(z)$;

iii) la struttura nota come Tridiagonal LFSR corrispondente alla matrice tridiagonale avente come sopra e sotto diagonali principali tutti 1 e polinomio caratteristico $p(z)$.

Le tre strutture hanno vantaggi e svantaggi che le rendono adatte a differenti applicazioni. In particolare, due proprietà, ossia casualità e complessità, si contrappongono, e tipicamente, per ottenere sequenze che manifestino buone proprietà di casualità, occorre aumentare la complessità dei circuiti, ossia il numero di operazioni binarie per bit generato.
Peraltro, tutte e tre le strutture consentono varianti che le rendono più adattate a scopi specifici, in particolare il cosiddetto controllo di clock, rende il profilo di complessità lineare delle sequenze generate quasi ottimale per applicazioni crittografiche.

Quantum key distribution and unconditionally secure keys

Dott. Matteo Canale, Università di Padova

10:05 - 10:20

Quantum key distribution, by leveraging the fundamental laws of quantum physics, allows two parties (Alice and Bob) to share a pair of unconditionally secure keys, on which a potential eavesdropper (Eve) has ideally no information. In order to distill such a pair of keys in a realistic environment, however, it is mandatory for Alice and Bob to post-process the raw keys they established through the quantum channel, both for correcting the errors that the quantum channel is likely to have introduced and for arbitrarily reducing the information that Eve actually has on the final keys. In this talk we will describe a practical "divide-et-impera" scheme for secret key agreement as applied to quantum key distribution and give some examples of practical solutions for each of its building blocks.

A survey on block ciphers

Dott. Anna Rimoldi, Università di Trento

10:20 - 10:35

We provide an introduction to symmetric encryption in general and to block ciphers in particular. We also outline some basic ideas about the security requirements that a good iterated block cipher should have.

Vulnerabilità dei protocolli SSL/TLS

Prof. Andrea Visconti, Università di Milano

10:55 - 11:20

I protocolli crittografici SSL/TLS sono soggetti ad una serie di vulnerabilità causate da errori di implementazione del protocollo. Un utente malintenzionato, sfruttando opportunamente queste vulnerabilità, può implementare attacchi Man-in-the-middle (MITM) durante la comunicazione client-server, minando la confidenzialità e/o l'integrità delle informazioni trasmesse in una sessione cifrata. In questa presentazione verranno introdotte tre vulnerabilità note in letteratura, le debolezze che un attaccante può sfruttare, e le necessarie contromisure da adottare per prevenire tali attacchi.

Enforcing Security Policies in Outsourced Environments

Dott. Asghar Rizwan, Università di Trento

11:20 - 11:35

The enforcement of security policies in outsourced environments is still an open challenge for the state-of-the-art policy-based systems. On the one hand, taking security decisions requires access to policies; on the other hand, these policies might leak private information about the sensitive data. In this talk, we address issue of enforcing security policies in outsourced environments while preserving confidentiality of policies.

OpenNET: un cluster altamente scalabile per la gestione di sistemi remoti e costruito con hardware di recupero

Dott. Lorenzo Nicolodi, Università di Bolzano

11:35 - 11:50

Nell'ultimo decennio, l'utilizzo di appliance sviluppati da aziende e installati presso i loro clienti finali è diventato sempre più frequente. Questo ha portato ad aumentare anche la frequenza con cui i tecnici hanno necessità di connettersi con questi appliance per manutenzione o per interventi di supporto al cliente, come alternativa agli interventi in loco. Quando invece il supporto remoto per un appliance è reso disponibile tramite Internet, sorgono nuovi problemi riguardanti la sicurezza dell'appliance, se questo è raggiungibile tramite un IP pubblico, oppure la possibilità stessa di raggiungerlo, se questo è protetto da un firewall e connesso ad una rete privata. Ogni azienda che si trova a dover gestire questi appliace in maniera centralizzata, finisce per sviluppare una soluzione ad-hoc, portando alla reimplementazione delle soluzioni che altre aziende hanno trovato ed utilizzato per risolvere il medesimo problema. Da una lato, una soluzione di questo tipo potrebbe richiedere uno sforzo considerevole per essere implementata e mantenuta e, dall'altro lato, potrebbe esser in grado di soddisfare solo i requisiti di quella specifica azienda. Attualmente, non esistono soluzioni né commerciali né open source, che mettono a disposizione un insieme di strumenti generici in grado di essere utilizzati in questo tipo di scenario. La mia tesi inizia con un'analisi dell'insieme dei problemi che un'azienda sperimenta quando si trova a gestire un certo numero di appliance, seguita poi dalla raccolta dei requisiti, portata a termine intervistando manager, tecnici e utenti di differenti aziende e con differenti livelli di conoscenze tecniche. Gli altri requisiti sono stati definiti basandomi sulla mia esperienza lavorativa. Partendo da questi requisiti, ho quindi cercato di risolvere ogni problema (o insieme di problemi) tenendo a mente che il mio obiettivo era quello di risolverli nella maniera più lineare, semplice e sicura possibile, creando un sistema che fosse relativamente semplice da installare e da amministrare. Considerando poi il fatto che spesso le aziende che iniziano un'attività che richiede l'utilizzo di OpenNET non hanno disponibilità di grandi capitali da investire, un'altro obiettivo del progetto era quello di fornire il servizio richiesto nella maniera più economicamente conveniente, senza per questo intaccarne l'affidabilità. Infine, ho costruito un ambiente virtuale dove ho iniziato lo sviluppo di OpenNET come un cluster di macchine Linux. Il risultato più interessante di questa fase sono gli script

di installazione, che sono in grado di installare automaticamente un nodo di un cluster, partendo da un certo numero di file di configurazione e da alcune opzioni di default. OpenNET è attualmente in fase di valutazione presso una ditta di Merano, che è interessata a miglioramenti e sviluppi futuri e che potrebbe diventare uno dei maggiori supporter di questo progetto.

A computational forensic methodology for malicious application detection on Android OS

Dott. Svetlana Voronkova, Università di Bolzano

11:50 - 12:05

E-discovery includes any process of searching, storing and securing digital information. Digital forensics is one of the least explored branches of e-discovery that examines how the extraction of digital evidence can aid in crime investigations and identification of potential suspects. Due to the growing popularity of smartphones, the field of mobile forensics - that is a part of digital forensics - gains more and more importance. However, many existing mobile forensic techniques cannot be (yet) fully applied to the Android OS, as its file system and architecture differ from already existing mobile platforms in many aspects. Moreover, Android provides access to a wide range of libraries and sophisticated functions that make the operating system very attractive to malicious software creators and increases the probability of its use in various illegal activities. This study presents a semi-automated mobile forensics methodology aimed at supporting a forensics examiner in detection of suspicious applications such as the ones that are generally considered as malware, i.e. those that might exploit sensible data stored on the mobile devices in a vulnerable way. The technique is based on the features of Android's security model, namely the set of standard permissions exposed by each application. The methodology relies on a set of more than 13000 safe applications, hosted on the Android Market and collected with AppAware, a specific tool for Android OS. The proposed system includes a web-based application for forensic a professional that allows to perform the detection of malicious applications on the chosen source and to manage the results of analysis. Another component is an Android application that presents the shorten version of detection report to the mobile device end user. The paper presenting this approach was submitted and accepted to the 4th International Workshop on Computational Forensics (IWCF), which took place in November 2010. The work presented has received a positive feedback.

Tecnica di oscuramento del segnale radio con chiave crittografica basata su coordinate spaziali

Dott. Mario Marcovecchio, Università di Firenze

12:05 - 12:20

Il sistema "Advanced Noise Loop" è una proposta di sicurezza intrinseca che utilizza il rumore termico, elemento univoco di un dispositivo e non riproducibile, per trasferire l?informazione. Esso si compone di tre stazioni fisse Alice che comunicano con un terminale mobile Bob, la cui posizione è univocamente determinata dai tempi di propagazione dei segnali provenienti dalle stazioni. Questo lo rende l?unico destinatario dell?informazione poiché la chiave per la decodifica dei messaggi risiede nella specifica posizione di Bob. Gli studi in caso di attacco rivelano che la presenza di un ascoltatore indesiderato non impedisce la corretta ricezione dell?informazione sui terminali autorizzati, né egli può in alcun modo ottenere l?informazione per intercettazione. In rari casi può provocare un Denial of Service, ma non ne verrebbe a conoscenza. Essendo totalmente immune dall?intercettazione il sistema risulta ottimale per scenari dove avviene lo scambio di chiavi di sicurezza.

Automated Security Analysis of Cryptographic Protocols

Dott. Alessandro Armando, Fondazione Bruno Kessler

12:20 - 12:35

Cryptographic protocols are communication protocols that, by means of cryptographic primitives, aim to provide security guarantees such as authentication of the participating agents and/or secrecy of some information (e.g. a session key). In spite of their apparent simplicity, security protocols are notoriously error-prone. Many published protocols have been implemented and deployed only to be found flawed years later. Quite interestingly, many attacks can be carried out without breaking cryptography. These attacks exploit weaknesses in the protocol that are due to the complex and unexpected interleavings of different protocol sessions as well as to the possible interference of malicious agents. For this reason, cryptographic protocols are a promising application domain for formal methods and model checking techniques in particular. In this talk I will provide a brief introduction to model checking of cryptographic protocols.

Unobservable intrusion detection based on call traces in paravirtualized systems

Prof. Marino Miculan, Università di Udine

12:35 - 13:00

In this talk we will present a non-invasive system for intrusion and anomaly detection, based on system call tracing in paravirtualized machines. System calls from guest user programs and operating systems are intercepted stealthy within Xen hypervisor, and passed to a detection system running in Dom0 via a suitable communication channel. Guest applications and machines are left unchanged, and an intruder on the virtual machine cannot tell whether the system is under inspection or not. Then, we present two detection algorithms: first, a statistical algorithm based on Stide, which we have verified experimentally to be fast and adequate, and a more recent development based on execution graphs model with data flow constraints.

Haruspex: analisi del rischio ICT con metodo Monte Carlo

Dott. Claudio Telmon, Università di Pisa

15:40 - 16:05

L'analisi del rischio di sicurezza in sistemi ICT si scontra spesso con difficoltà nell'ottenere valutazioni credibili sulla probabilità di successo di attività ostili, specialmente quando si considerino attacchi multi-step in cui una minaccia utilizzi più attacchi elementari per raggiungere i propri obiettivi. Questa difficoltà ha come conseguenza la soggettività di molti risultati. Le minacce intelligenti sono particolarmente difficili da affrontare con un approccio statistico, perché a differenza di un guasto sono in grado di adattare il proprio comportamento al contesto ed alle contromisure messe in atto. Haruspex simula con il metodo Monte Carlo il comportamento di una minaccia intelligente all'interno di un sistema in cui fattori non predicibili, come la scoperta di nuove vulnerabilità, sono modellati con opportune distribuzioni di probabilità. Il simulatore permette quindi di ottenere i valori statistici necessari per una valutazione più oggettiva del rischio e un'ottimizzazione dell'efficacia e del costo delle contromisure.

A new bound on the size of linear codes

Dott. Emanuele Bellini, Università di Trento

16:05 - 16:20

The problem of finding a bound for the size of a code is a central problem in coding theory. We present two new bounds for the size of a systematic code. These bounds are independent of several known bounds on non-linear codes and in some cases are the best known. In particular, we often beat the Griesmer bound, which holds for linear codes, which are a subset of systematic codes.
Joint work with Prof. M. Sala and Dott. E. Guerrini.

Risultati sulla decodifica dei codici da varietà affine

Dott. Chiara Marcolla, Università di Trento

16:30 - 16:35

I general error locator polynomials sono polinomi in grado di decodificare ciascuna sindrome correggibile di un codice lineare. E' dimostrata l'esistenza di questi polinomi per i codici ciclici e per una grande parte dei codici lineari. In questo talk vediamo un'estensione multidimensionale dei polinomi locatori per i codici da varietà affine e analizziamo un esempio interessante: i codici Hermitiani. Per fare ciò avremo bisogno di una classe speciale di ideali zero - dimensionali, che può essere considerata una generalizzazione degli ideali stratificati.

Curve massimali definite su campi finiti di ordine piccolo

Dott. Irene Platoni, Università di Trento

16:35 - 16:50

Mostreremo che esiste un'unica curva massimale di genere 7, definita sul campo finito con 49 elementi, a meno di equivalenza birazionale. Questo era il primo problema aperto di classificazione di curve massimali che si presentava, poiché le curve massimali definite su campi finiti con meno di 49 elementi, così come le curve massimali definite su campi finiti con 49 elementi, di genere maggiore di 7, sono state precedentemente classificate. Un ruolo significativo hanno avuto alcune ricerche esaustive al computer.

Codici AG generalizzati da curve massimali

Dott. Marco Calderini, Università di Trento

16:50 - 17:05

La teoria dei codici correttori di errori costruiti da curve algebriche definite su un campo finito è stata iniziata da Goppa, nel 1980, con i così detti codici algebrico-geometrici (AG). La costruzione di tali codici usa i punti razionali di una curva proiettiva non singolare, cioè i punti che hanno coordinate nel campo finito su cui è definita la curva.
Nel 1999 Xing, Niederrieter e Lam introducono un nuovo metodo per costruire codici lineari da curve algebriche. La loro costruzione utilizza, oltre ai punti razionali, anche i punti a coordinate in estensioni del campo base e il processo di concatenazione di codici. Questi codici sono detti algebrico-geometrici generalizzati (GAG), in quanto vanno a generalizzare la costruzione di Goppa. Attraverso la costruzione dei codici GAG associati a curve algebriche massimali, cioè curve per cui vale l'uguaglianza nella disuguaglianza di Hasse-Weil, è possibile ottenere codici lineari con parametri migliori rispetto a quelli dei codici presenti nelle tabelle MinT. Inoltre con i codici GAG è possibile determinare sequenze esplicite di codici lineari asintoticamente buoni.

Geometria dei two-point codes su curva Hermitiana

Dott. Alberto Ravagnani, Università di Trento

17:15 - 17:30

In questo intervento si discute la geometria algebrica dei codici two-point su curva Hermitiana, descrivendo le parole di peso minimo di alcuni dei loro codici duali.

Ricerca di codici estremali autoduali di lunghezza 72

Dott. Martino Borello, Università di Milano-Bicocca

17:30 - 17:45

In questo seminario presenteremo il problema dell'esistenza di un codice autoduale di parametri $[72, 36, 16]$, posto da Sloane nel 1973 e tuttora irrisolto. Recenti risultati mostrano che il gruppo degli automorfismi di un ipotetico codice con tali caratteristiche è molto piccolo, in particolare la sua cardinalità non supera 24, e gli automorfismi possibili hanno ordine 1,2,3,4,5,6 o 12. Mostreremo alcuni risultati riguardanti gli automorfismi di ordine 6, a partire dallo studio dei codici da loro fissati.