PENGGUNAAN TEKNIK *FUZZING* UNTUK MENEMUKAN CELAH KEAMANAN PADA *PROPRIETARY NETWORK PROTOCOLS* :

Studi Kasus *Network Protocols* Pada Sistem ATM (*Automated Teller Machine*)

TESIS

Oleh :

ARIF JATMOKO

0811600808

PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

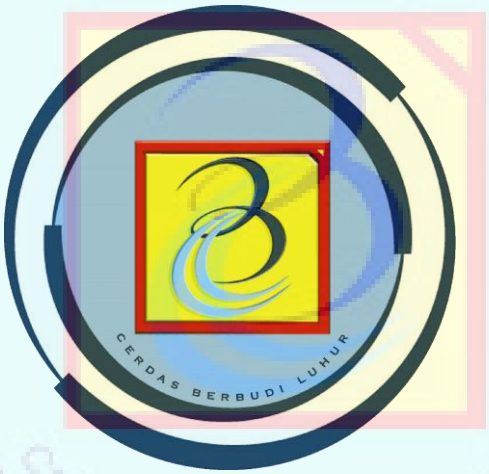
JAKARTA
2012

PENGGUNAAN TEKNIK *FUZZING* UNTUK MENEMUKAN CELAH KEAMANAN PADA *PROPRIETARY NETWORK PROTOCOLS* :

Studi Kasus *Network Protocols* Pada Sistem ATM (*Automated Teller Machine*)

TESIS

Diajukan sebagai salah satu persyaratan
untuk mendapatkan gelar Magister Ilmu Komputer (M.Kom)



Oleh :

ARIF JATMOKO

0811600808

PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

JAKARTA
2012

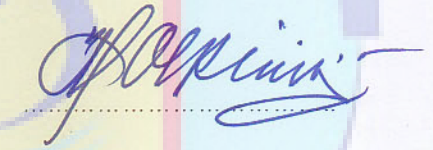
PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

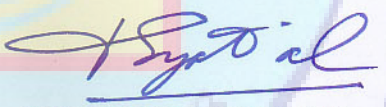
LEMBAR PENGESAHAN

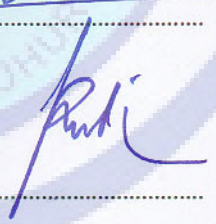
Nama	:	Arif Jatmoko
NIM	:	0811600808
Konsentrasi	:	Manajemen Fungsi Sistem Informasi
Jenjang Studi	:	Strata 2
Judul	:	Penggunaan Teknik *Fuzzing* Untuk Menemukan Celah Keamanan Pada *Proprietary Network Protocols* : Studi Kasus *Network Protocols* Pada Sistem ATM (*Automated Teller Machine*)

Jakarta, 10 Agustus 2012

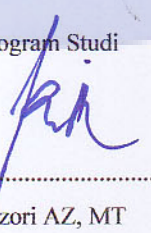
Tim Penguji — Tanda Tangan :

Ketua,
Dr. Moedjiono, M.Sc ..... 

Anggota,
Hadi Syahrial, MM, M.Kom ..... 

Pembimbing,
Dr. Ir. Nazori AZ, MT ..... 

Ketua Program Studi



.....

Dr. Ir. Nazori AZ, MT

PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PERNYATAAN

Saya yang bertanda tangan di bawah ini :

Nama : ARIF JATMOKO

NIM : 0811600808

Program Studi : MAGISTER ILMU KOMPUTER

Menyatakan bahwa tesis yang berjudul :

PENGGUNAAN TEKNIK FUZZING UNTUK MENEMUKAN CELAH KEAMANAN PADA PROPRIETARY NETWORK PROTOCOLS : STUDI KASUS NETWORK PROTOCOLS PADA SISTEM ATM (AUTOMATED TELLER MACHINE)

1. Merupakan hasil karya tulis ilmiah sendiri dan bukan merupakan karya yang pernah diajukan untuk memperoleh gelar akademik oleh pihak lain.
2. *Saya ijinkan untuk dikelola oleh Universitas Budi Luhur sesuai dengan norma hukum dan etika yang* berlaku.

Pernyataan ini saya buat dengan penuh tanggung jawab dan saya bersedia menerima konsekuensi apapun sesuai aturan yang berlaku apabila di kemudian hari pernyataan ini tidak benar.

Jakarta, 10 Agustus 2012

Arif Jatmoko

ABSTRAK

Sistem ATM (Anjungan Tunai Mandiri) merupakan salah satu layanan perbankan yang tergolong paling kritis. Adanya *security bugs* (celah kelemahan) di dalamnya dapat berisiko besar bagi pihak bank dan nasabahnya secara umum. Penggunaan *proprietary protocols* ketimbang *open standard* dalam implementasi sistem ATM semakin menyulitkan identifikasi *security bugs* yang mungkin terdapat di dalamnya. Dalam *proprietary protocols* seperti sistem ATM, dokumentasi teknis yang mencakup spesifikasi dan format protokol sangat terbatas dan sulit didapatkan. Sementara itu, belum pernah terdapat publikasi tentang *security bugs* itu sendiri dalam sistem ATM, padahal fakta menunjukkan bahwa terdapat pemberitaan tentang adanya pelaku kriminal yang berhasil mengeksploitasi sistem ATM ini. Salah satu teknik pendekatan untuk menemukan *security bugs* jenis *memory corruptions* adalah *fuzz testing* atau *fuzzing*. Teknik ini sangat efektif, namun si peneliti harus memiliki pemahaman yang mendalam terhadap spesifikasi teknis dan format protokol sistem yang diuji dimana hal ini tidak memungkinkan pada *proprietary protocols* sistem ATM. Beberapa penelitian sebelumnya telah berhasil membuktikan deteksi *security bugs* secara otomatis pada *proprietary protocols* sistem SCADA dengan pendekatan *proxy fuzzing* dan *inline fuzzing*. Namun demikian, kedua pendekatan ini cenderung bersifat *intrusive* karena memodifikasi sistem infrastruktur sehingga dimungkinkan terjadinya kerusakan sistem ATM yang diuji. Tesis ini menggunakan metode *bio-informatics* semi-otomatis untuk identifikasi format, *field*, dan spesifikasi teknis lainnya pada *proprietary protocols* sistem ATM. Hasil identifikasi tersebut selanjutnya digunakan sebagai dasar penentuan *input* dan penyusunan *skeleton* untuk proses *fuzzing* menggunakan `Sulley` *framework*.

Hasil *fuzzing* yang dilakukan terhadap lima sistem aplikasi ATM menunjukkan adanya *security bug* pada tiga diantaranya. Hasil ini sesuai dengan hipotesis penelitian bahwa terdapat *memory corruption bugs* dalam sistem ATM, namun perlu dilakukan analisis lebih lanjut untuk mengetahui jenis *bug* tersebut dan dampak yang ditimbulkan, misalnya sebab dan akibat adanya *bug*, *exploitability*, dan lainnya. Analisis terhadap jenis *bug* dan dampaknya diluar lingkup penelitian, dan secara etika merupakan kewajiban pihak pabrikan untuk melakukan serangkaian *software security audit* secara mendalam. Temuan ini diharapkan dapat menjadi dasar penyusunan mitigasi risiko bagi pihak bank pengelola ATM sehingga tidak terjadi penyalahgunaan transaksi ATM oleh pihak yang tidak bertanggung jawab.

Kata kunci : *fuzzing*, *proprietary protocols*, ATM, *reverse engineer*, `sulley`

ABSTRACT

ATM (Automated Teller Machine) system is one of the mission-critical banking services. If such security bugs exist in the systems, there would be major risks for bank or ATM provider and its customers. The implementation of proprietary protocols in ATM systems instead of open standard protocols has increased complexity the detection of possible security bugs. Accesses to technical documentations including specification and protocol format for proprietary systems like ATM are not publicly available, and in some cases, very restricted. For the time being, study literature has no finding about security bugs in the ATM systems, while the fact was ATM systems proved to be exploitable by criminals. One of the best approach to detect security bugs is called fuzzing or fuzz testing, which is capable to detect bug categorize as memory corruption bugs. This approach has proven very effective if the tester having depth knowledge about protocol specifications, which is unavailable in the case. Using novel approach like proxy fuzzing and inline fuzzing, previous studies has succeeded automatically revealed some memory corruption bugs in proprietary protocols SCADA with zero knowledge of the tester. However, these approaches are tend to intrusive by modifying system infrastructure's target being tested that may damage ATM systems. This thesis research is using semi-automatic bio-informatics method to identify protocol format, field, and other technical specifications in proprietary protocols ATM systems. The identified results are then used as basis for mutated inputs and build skeleton fuzzer in `Sulley` *fuzzing framework.*

The fuzzing result has found six security bugs from five ATM software tested, which is answering research hypothesis. However, this finding should further evaluated through depth software security audit by software manufacturer i.e. what causes and impact of the bugs, exploitability, etc. These are beyond the scope of the thesis. Based on this finding results, ATM provider should be able to develop risk mitigation strategy to prevent misuse of ATM systems being exploited by malicious users.

Keywords : fuzzing, software testing, ATM, *reverse engineer,* `sulley`

KATA PENGANTAR

Dengan mengucapkan puji dan syukur kehadirat Allah SWT yang telah melimpahkan rahmat dan karunia-NYA serta selawat dan salam ke atas pangkuan Rasullullah SAW, sehingga penulis telah dapat menyelesaikan penulisan naskah Tesis dengan judul ”PENGGUNAAN TEKNIK FUZZING UNTUK MENEMUKAN CELAH KEAMANAN PADA *PROPRIETARY NETWORK PROTOCOL* : STUDI KASUS *NETWORK PROTOCOL* PADA SISTEM ATM (*AUTOMATED TELLER MACHINE*)”. Tesis ini disusun guna diajukan dan disajikan dihadapan para penguji dan pembimbing dengan harapan dapat disetujui untuk segera dilanjutkan dengan tahap penelitian sesuai persyaratan tesis dalam mendapatkan gelar Master Ilmu Komputer (MKOM), Program Pascasarjana Teknologi Informasi di Universitas Budi Luhur, Jakarta.

Pada kesempatan ini penulis mengucapkan terima kasih yang sebesar-besarnya kepada semua pihak yang telah banyak membantu, terutama :

1. Bapak Dr. Moedjiono, MSc., selaku Direktur Program Pascasarjana Universitas Budi Luhur.
2. Bapak Dr. Ir. Nazori AZ, MT., selaku Ketua Program Studi Magister Ilmu Komputer Program Pascasarjana Universitas Budi Luhur dan sekaligus dosen pembimbing utama yang telah banyak membantu dan memberikan arahan serta bimbingannya dalam penelitian ini.
3. Seluruh dosen beserta sivitas akademika Program Pascasarjana Universitas Budi Luhur yang telah memberikan layanan dan dukungan dalam proses penyusunan penelitian ini.
4. Seluruh rekan-rekan kerja tim ATM Monitoring yang telah membantu menyediakan data, rekan-rekan di ATM Application Support yang membantu menyediakan *testing environment*, serta semua rekan-rekan lain yang tidak disebutkan disini.
5. Seluruh pihak yang telah membantu penulis dalam menyelesaikan penelitian ini, pakar *fuzzing* Pedram Amini dan Aaron Portmoy yang telah memberikan pencerahan tentang `Sulley`, dan Michael ‘`Peach`’ Eddington untuk pencerahan tentang `Peach` *fuzzer*. Selama riset, penulis banyak sekali mendapat pengetahuan

baru tentang protokol dan pemodelannya dari tim `Netzob` Frederic Guihery dan Georges Bossert.

6. Istri, anak-anakku, ibunda, dan ayahanda tercinta yang sabar memberikan motivasi selama proses kuliah, belajar, riset, hingga penyelesaian tesis ini. Tanpa dukungan, bantuan, dan doa terijabah, tesis ini tidak mungkin dapat selesai pada waktunya.

Akhir kata, penulis berharap agar tesis ini dapat bermanfaat bagi semua pihak yang membutuhkan.

Jakarta, Agustus 2012

Penulis

DAFTAR ISI

halaman

DAFTAR GAMBAR

Gambar halaman

DAFTAR TABEL

Tabel halaman

DAFTAR LAMPIRAN

DAFTAR PUSTAKA

[AlephOne 1996] AlephOne. "**Smashing The Stack For Fun And Profit**". Phrack Magazine, Vol 7, Issue 49, November 08, 1996.

[Aitel 2002] Aitel, Dave. **The Advantages of Block-Based Protocol Analysis for Security Testing**, February 4, 2002. New York. www.immunitysec.com/downloads/advantages_of_block_based_analysis.txt

[Amini 2007] Amini, Pedram. **Mostrame la guita! Adventures in buying vulnerabilities.** https://docs.google.com/present/view?id=dcc6wpsd_20ghbpjxcr

[Anley dkk 2007] Anley, Chris, John Heasman, Felix "FX" Linder, Gerardo Richarte, **The Shellcoder's Handbook: Discovering and Exploiting Security Holes**. Second Endition. Wiley Publishing, Inc., Indianapolis, 2007.

[Bank Indonesia 2011]. Bank Indonesia. "**Implementasi Teknologi Chip dan Penggunaan Personal Identification Number pada Kartu ATM dan/atau Kartu Debet yang diterbitkan di Indonesia**". Surat Edaran Bank Indonesia No. 13/ 22 /DASP. Bank Indonesia. 2011. http://www.bi.go.id/web/id/Peraturan/Sistem+Pembayaran/se_132211.htm. (Diakses tanggal 18 Februari 2012).

[Batiz-Lazo 2007] Batiz-Lazo, Bernardo. "**Emergence and Evolution of Proprietary ATM Networks in the UK, 1967-2000**". Paper presented at the 2007 Annual Meeting of the Business History Conference, MPRA (Munich Personal RePEc Archive) Paper, No. 3689. 2007.

[Bratus dkk 2008] Bratus Sergey, Axel Hansen, Anna Shubina. "**LZfuzz: A Fast Compression-based Fuzzer for Poorly Documented Protocols**". Dartmouth Computer Science Technical Report, TR2008-634, Department of Computer Science, Dartmouth College, Hanover. 2008.

[Datta 2010] Datta, Abhisek. "**WirePlay : An Approach to Almost Blind Fuzzing**". NullCon GOA 2010. 2010. http://nullcon.net/nullcon2010presentation/Abhisek_wireplay_nullcon_2010.pdf, diakses tanggal 30 Maret 2012.