System Security Requirement untuk Perancangan *Intelligent Public Transport* pada Sistem Pembayaran Elektronik Angkutan Kota

Khairani Ummah - 23215138

May 23, 2016

Abstrak

Salah satu contoh permasalahan tarif pada transportasi umum adalah tarif yang kontradiktif pada angkutan kota. Untuk jarak tempuh yang sama, antar angkot dapat memberlakukan tarif yang berbeda. Dalam mengatasi permasalahan tersebut, telah diusulkan sebuah rancangan sistem pembayaran elektronik angkutan kota. Namun, dalam rancangan tersebut belum melibatkan aspek *security*. Oleh karena itu, akan dilakukan proses *re-engineering* sistem dengan memasukkan aspek keamanan. Untuk melakukan proses *re-engineering*, digunakan NIST SP 800-160 sebagai panduan *system security engineering*.

Pada makalah ini akan dibahas *security requirement* dengan menggunakan metodologi *security requirement elicitation*. *Problem frames* yang digunakan pada *system modeling* adalah *system requirement* yang diturunkan dari *stakeholder requirement*. Identifikasi ancaman dan kerentanan yang dilakukan menggunakan STRIDE threat list. Identifikasi dan analisis yang dilakukan telah menghasilkan daftar 14 poin *security requirement* untuk Sistem Pembayaran Elektronik Angkutan Kota.

Kata kunci: *security requirement elicitation*, STRIDE, sistem pembayaran elektronik, angkutan kota, NIST SP 800-160

Daftar Isi

Daftar Gambar

Daftar Tabel

Bab I

Pendahuluan

I.1 Latar Belakang

Terdapat berbagai jenis kendaraan umum di Indonesia. Namun banyaknya jenis kendaraan umum ini belum berhasil mengurangi permasalahan seputar transportasi yang ada, terlebih di daerah perkotaan. Pengguna kendaraan pribadi masih banyak dan tak banyak yang mau untuk berpindah menggunakan transportasi umum. Hal ini salah satunya disebabkan oleh pelayanan dan kondisi angkutan umum yang belum memenuhi harapan masyarakat dan tarif yang kontradiktif. Salah satu contoh permasalahan tarif yang kontradiktif terjadi pada angkutan kota. Untuk jarak tempuh yang sama, antarangkot dapat memberlakukan tarif yang berbeda.

Untuk mengatasi permasalahan tarif yang kontradiktif pada angkutan kota tersebut, telah diusulkan sebuah rancangan sistem pembayaran elektronik angkutan kota. Rancangan tersebut tertuang pada penelitian yang berjudul Rancang Bangun Purwarupa Sistem Pembayaran Elektronik Angkutan Kota, Studi Kasus: Kota Bandung. Perancangan yang dilakukan menghasilkan sistem pembayaran elektronik untuk angkutan kota dengan menggunakan kartu NFC dengan penambahan tarif berbasiskan area *checkpoint* dengan koneksi ke server melalui Wifi. Pada sistem ini, penumpang melakukan pemindaian kartu NFC saat naik dan turun angkot. Tarif bertambah setiap angkot melewati area *checkpoint* dan tarif dibayarkan dengan pemotongan saldo yang dimiliki penumpang secara otomatis saat penumpang turun dari angkot. Sistem ini memungkinkan standar tarif untuk jarak yang sama pada setiap angkot dengan trayek yang sama.

Perancangan yang sebelumnya dilakukan, menggunakan metode *Design Science Research Methodology* (DSRM) *for Information System Research* oleh Peffers et al untuk proses *system engineering*. Dalam proses *system engineering*, terdapat aspek yang perlu dipertimbangkan, yaitu aspek *security*. Namun, pada

proses *system engineering* sistem pembayaran elektronik angkutan kota yang dilakukan sebelumnya, aspek *security* belum menjadi pertimbangan dalam perancangan sistem. Berdasarkan PP RI No.82 tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik terdapat pernyataan bahwa keamanan informasi wajib diselenggarakan. Oleh karena itu, aspek *security* menjadi sebuah kebutuhan dalam *system engineering*. Sehingga perlu dilakukan proses *re-engineering* untuk sistem pembayaran elektronik angkutan kota ini agar dapat menyelenggarakan keamanan informasi pada sistem yang dibangun.

Pada Mei 2014, NIST mempublikasikan sebuah *Initial Public Draft* dari *Special Publication* (SP) 800-160 mengenai *System Security Engineering*: *An Integrated Approach to Building Trustworthy Resillient System*. Pada NIST SP 800-160 tersebut terdapat panduan berupa langkah-langkah untuk melaksanakan *system engineering* dengan memasukkan aspek keamanan dan membuat sistem yang tahan terhadap serangan. NIST SP 800-160 dibuat dengan tujuan untuk mengintegrasikan proses *security engineering* kedalam proses *system engineering*. Dengan demikian, NIST SP 800-160 ini dapat digunakan sebagai panduan system *security engineering* pada proses *re-engineering* sistem pembayaran elektronik angkutan kota.

Terkait angkutan perkotaan, sistem yang akan dibuat ini hendak mengikuti *intelligent public transport*. *Intelligent Public Transport* (IPT) merupakan aplikasi teknologi informasi dan komunikasi untuk jaringan kendaraan umum untuk meningkatkan level layanan dan efisiensi [3]. Pada dokumentasi penelitian dari Enisa yang berjudul *Cyber Security and Resilience of Intelligent Public Transport*, dibahas mengenai kebutuhan untuk mengamankan IPT. Kebutuhan akan pengamanan IPT dituangkan dengan menjabarkan ancaman, kerentanan, dan risiko dari IPT pada dokumen tersebut.

Berdasarkan kebutuhan akan aspek security pada proses *system engineering* sistem pembayaran elektronik angkutan kota, pada makalah ini akan dibahas tahap awal proses *re-engineering* yaitu dengan membuat *security requirement* untuk sistem pembayaran elektronik angkutan kota. Dengan berbasis pada ancaman (*threats*) yang ada, maka kebutuhan akan pengamanan akan dibentuk sehingga menghasilkan *security requirement*. Metodologi untuk melakukan *security requirement elicitation* menggunakan metodologi yang dibuat oleh Hassan El-Hadary dan Sherif El-Kassas [2].

I.2 Permasalahan

Berdasarkan latar belakang yang telah dijabarkan pada bagian sebelumnya, pada makalah ini permasalahan yang akan diselesaikan adalah apa saja *system security requirement* dari sistem pembayaran elektronik angkutan kota.

I.3 Tujuan

Tujuan dibuatnya makalah ini adalah untuk mengetahui kebutuhan keamanan pada sistem pembayaran elektronik sehingga dapat dilakukan proses *re-engineering* dengan kebutuhan sistem yang telah ditambahkan dengan kebutuhan keamanan. Dengan demikian, dapat dibuat rancangan sistem pembayaran elektronik angkutan kota yang lebih tahan terhadap serangan.

I.4 Batasan Masalah

Pada pembuatan makalah ini, terdapat batasan masalah antara lain:

1. *Stakeholder requirement* yang diturunkan masih berdasarkan analisis dari penelitian sebelumnya, belum berupa *survey* lapangan
2. *Abuse Frames* (AF) yang digunakan adalah dengan menggunakan kategori ancaman STRIDE (*spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege*)
3. *Problem Frames* (PF) yang digunakan adalah *system requirement* yang diturunkan dari *stakeholder requirement*
4. Tidak semua kebutuhan keamanan dari IPT yang diturunkan menjadi *security requirement*

Bab II

Tinjauan Pustaka

II.1 Sistem Pembayaran Elektronik Angkutan Kota [1]

Pada penelitian yang dilakukan sebelumnya telah dirancang dan dibangun purwarupa sistem pembayaran elektronik angkutan kota. Perancangan yang dilakukan menghasilkan sistem pembayaran elektronik untuk angkutan kota dengan menggunakan kartu NFC dengan penambahan tarif berbasiskan area checkpoint dengan koneksi ke server melalui Wifi. Pada sistem ini, penumpang melakukan pemindaian kartu NFC saat naik dan turun angkot. Tarif bertambah setiap angkot melewati area checkpoint dan tarif dibayarkan dengan pemotongan saldo yang dimiliki penumpang secara otomatis saat penumpang turun dari angkot. Sistem ini memungkinkan standar tarif untuk jarak yang sama pada setiap angkot dengan trayek yang sama.

II.1.1 Kebutuhan *Stakeholder*

Berdasarkan penelitian yang telah dilakukan, stakeholder yang terlibat dalam sistem pembayaran angkutan kota mencakup penumpang, pengemudi, dan pemilik angkot. Kebutuhan stakeholder terkait sistem transportasi angkutan kota ini dapat dilihat pada Tabel II.1 berikut ini.

II.1.2 Desain Sistem Pembayaran Elektronik Angkutan Kota

Pada sistem pembayaran elektronik angkutan kota, untuk alat pembayaran elektronik akan digunakan NFC Card. Koneksi dengan internet dilakukan dengan menggunakan Wifi. Pengukuran jarak angkot dilakukan dengan sistem perhitungan per area dengan perubahan atau penambahan tarif terjadi saat active

Tabel II.1: Kebutuhan *Stakeholder*

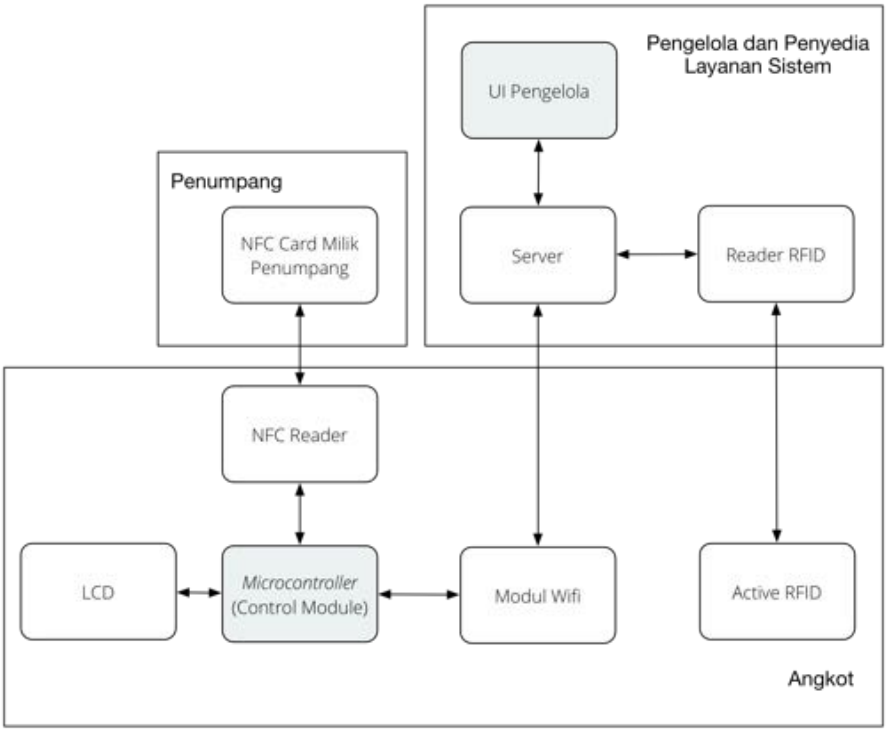
Stakeholder	Kebutuhan
Penumpang Angkot	Dapat melakukan transaksi dengan cepat
	Dapat membayar tarif yang sesuai dengan jarak tempuh
Pengemudi Angkot	Mendapatkan tarif yang sesuai dengan jarak tempuh
	Mengetahui jumlah pendapatan
Pemilik (Pengelola) Angkot	Mendapatkan setoran dari pengemudi angkot sesuai dengan kesepakatan
	Mengetahui pendapatan supir angkot

RFID angkot terbaca oleh reader pada daerah checkpoint.

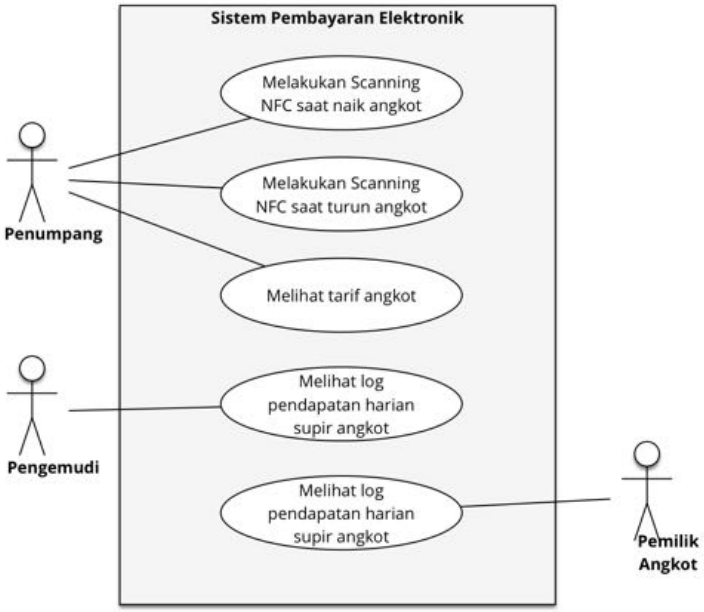
Dapat dilihat pada Gambar II.1 bahwa sistem terdiri dari 3 bagian yaitu bagian untuk penumpang, angkot, dan pengelola dan penyedia layanan sistem. Dari desain sistem ini, software yang akan dibuat antara lain pada Microcontroller dan UI pengelola. Untuk desain software lebih dalam akan dijelaskan pada subbab berikutnya. Pada bagian angkot terdapat komponen Microcontroller, LCD, NFC Shield, Wifi Shield, Battery, Active RFID. Pada bagian penumpang terdapat komponen NFC Card milik penumpang. Sedangkan pada bagian pengelola dan penyedia layanan sistem terdapat UI pengelola, database, server, dan reader untuk active RFID.

Pada sistem pembayaran elektronik ini, terdapat perubahan aktivitas setiap stakeholder. Aktivitas yang dilakukan oleh para stakeholder dapat dilihat pada diagram use case seperti pada Gambar II.2 di bawah ini. Diagram ini menggambarkan penumpang dapat melakukan scanning NFC Card pada saat naik dan turun angkot, serta melihat tarif angkot. Pengemudi dan pemilik angkot dapat melihat log transaksi harian dari angkutan kota yang bersangkutan.

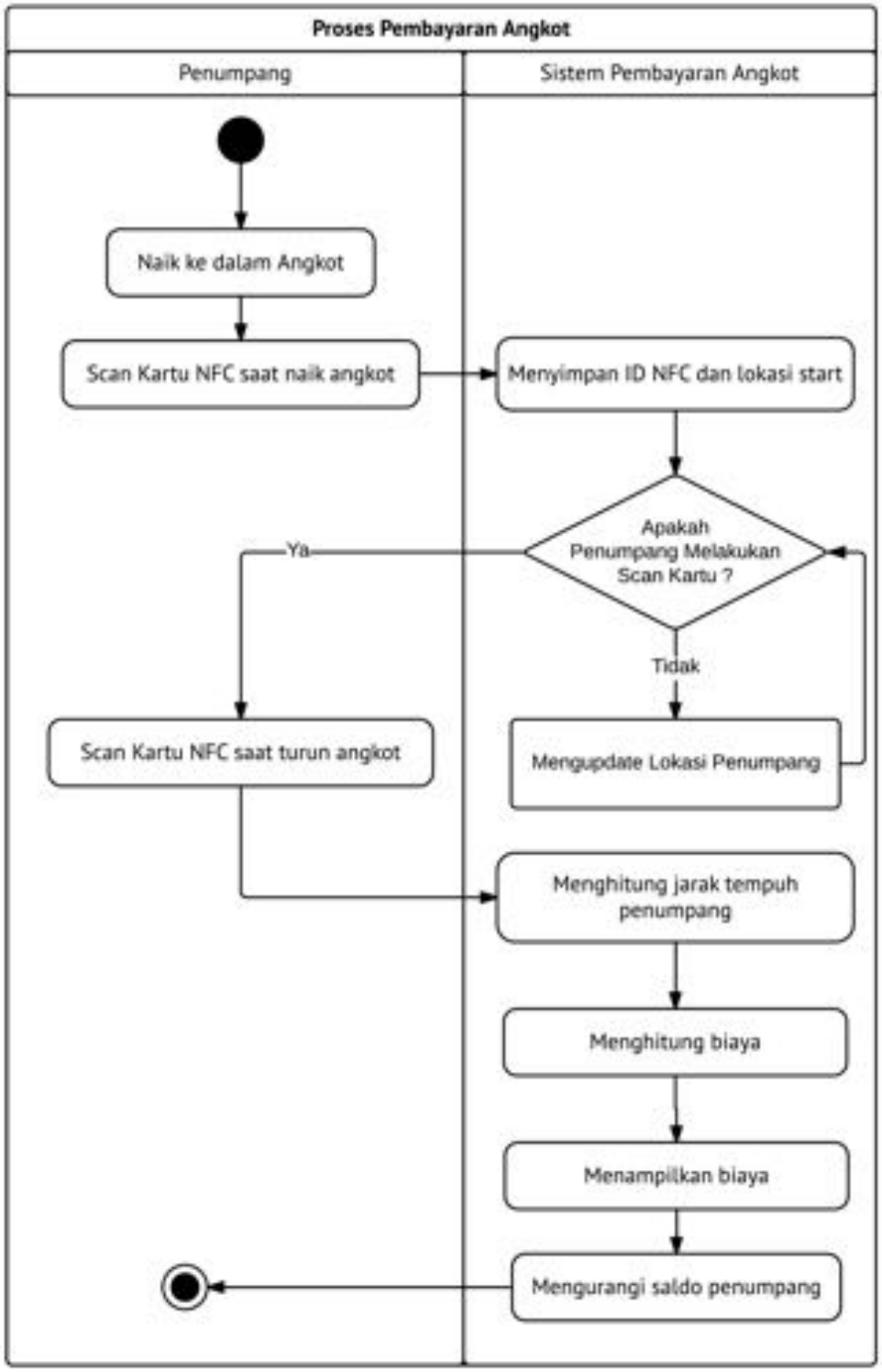
Untuk proses pembayaran angkot dapat dilihat seperti pada activity diagram pada Gambar II.3. Proses ini diawali dengan penumpang masuk ke dalam angkot dan melakukan scanning NFC card. Kemudian sistem akan membaca dan menyimpan ID penumpang serta mengimpan lokasi start. Setelah itu sistem akan memeriksa apakah penumpang melakukan pemindaian kartu atau tidak. Jika tidak, maka sistem akan meng-update lokasi penumpang. Jika ya, maka sistem akan menghitung jarak tempuh antara posisi start dengan checkpoint-checkpoint yang telah dilewati. Kemudian sistem akan menghitung biaya keseluruhan dan menampilkan biaya pada LCD yang tersedia. Setelah itu, sistem akan memotong saldo penumpang yang disimpan pada server.



Gambar II.1: Desain Sistem Pembayaran Elektronik Angkutan Kota



Gambar II.2: Use Case Diagram



Gambar II.3: Activity Diagram Pembayaran Angkot

II.2 NIST SP 800-160

National Institute of Standards and Technology (NIST) mempublikasikan *initial public draft* dari NIST *Special Publication* (SP) 800-160 pada Mei 2014 [5]. NIST SP 800-160 ini membahas S*ystem Security Engineering: An Integrated Approach to Building Trustworthy Resilient System*. Publikasi ini membahas aksi yang dibutuhkan untuk membangun infratruktur IT yang lebih *defensible* dan *survivable*. Sasaran utama dari dari publikasi ini adalah menunjukkan isu keamanan dari kebutuhan *stakeholder* dan kebutuhan proteksi, dan menggunakan proses organisasi yang ada untuk memastikan bahwa *requirement* terpenuhi dari awal dan sepanjang *life cycle* sistem. Tujuan dari publikasi ini ada 5 (lima), antara lain:

1. Untuk menyediakan pernyataan yang lengkap (*comprehensive statement*) mengenai disiplin *system security engineering*, prinsip-prinsip, konsep, dan aktivitasnya
2. Untuk membantu perkembangan *mindset* yang sama dalam menyediakan keamanan pada sistem apapun, terlepas dari lingkup, ukuran, kompleksitas, atau tahapan pada *system life cycle*
3. Untuk meningkatkan bidang *system security engineering* dengan menyebarkannya sebagai sebuah disiplin yang dapat diaplikasikan dan dipelajari
4. Untuk mendemonstrasikan bagaimana proses *system security engineering* dapat diitegrasikan secara efektif pada proses *system engineering*
5. Sebagai basis untuk pengembangan program edukasi dan pelatihan, termasuk pengembangan sertifikasi individu dan kriteria penilaian profesional lainnya

Terdapat 11 proses *system security engineering*, antara lain:

1. *Stakeholder Requirement Definition Process*
2. *Requirements Analysis Process*
3. *Architectural Design Process*
4. *Implementation Process*
5. *Integration Process*
6. *Verification Process*
7. *Transition Process*
8. *Validation Process*

9. *Operation Process*
10. *Maintenance Process*
11. *Disposal Process*

II.3 Kebutuhan Pengamanan *Intelligent Public Transport*

Intelligent Public Transport (IPT) merupakan aplikasi teknologi informasi dan komunikasi untuk jaringan kendaraan umum untuk meningkatkan level layanan dan efisiensi. Kebutuhan pengamanan *intelligent public transport* fokus pada ancaman, kerentanan, dan risiko yang dihadapi oleh jaringan dan operator IPT serta dampaknya pada bisnis dan sosial. Berikut definisi dari ancaman, kerentanan, dan risiko yang dimaksud [3]. Daftar ancaman dari IPT dapat dilihat pada tabel 2.2

- Ancaman (*threat*): penyebab yang potensial pada sebuah kejadian yang dapat membahayakan system atau organisasi IPT
- Kerentanan (*vulnerability*): kelemahan pada *asset* IPT yang dapat dieksploitasi dengan ancaman yang ada
- Risiko (*risk*): potensi bahwa ancaman yang diberikan dapat berhasil mengeksploitasi kerentanan pada asset IPT dan membahayakan bisnis dan/atau *society* secara keseluruhan

II.4 Metodologi *Security Requirement Elicitation*

Tujuan utama dari metodologi ini adalah untuk membantu *developer* dalam merumuskan *security requirement*. Pada metodologi ini digunakan *problem frames*. Problem frames digunakan untuk mendeskripsikan masalah dalam *software development*. Metodologi ini bertujuan untuk mengidentifikasi *security requirement* dengan pengetahuan keamanan sebelumnya melalui *security catalog*. *Security catalog* berisi *problem frame* (PF) *model* untuk ancaman (*threats*) dan *security requirement* yang memenuhinya. Ancaman dimodelkan dengan menggunakan *abuse frame* (AF), sedangkan *security requirement* dimodelkan dengan *security problem frames* (SPF) *[2]*.

Metodologi melakukan iterasi dengan langkah-langkah berikut:

1. *System modeling*
2. *Assets identification*

Tabel II.2: Ancaman (*Threats*) pada IPT [3]

Type	**Physical and large scale attacks**
	Terorism dan/atau serangan yang didukung negara
	Penggunaan dan/atau akses yang tidak terotorisasi (unauthorised use and/or access)
	Vandalism dan/atau ketidakpatuhan sipil
	Violence and/or shooting within sites
	Pencurian data dan/atau infrastruktur
Type	**Act of nature / environmental incidents**
	Bencana alam
	Bencana lingkungan
Type	**Accidental errors/malfunctions/failures**
	Hardware failure and/or malfunction
	Software failure and/or malfunctions
	Hilangnya integritas data atau informasi (Sensitif)
	Configuration errors
Type	**Disruption and/or outages**
	Interruption and/or disruption of electrical supply
	Interruption and/or disruption of frequency
	Strike
Type	**Nefarious activity /abuse**
	Distributed Denial of Service attacks (DDoS)
	Manipulation of hardware and/or software
	Malware and viruses
	Tempering and/or alteration of data including insertion of information
	Hacking of wireless , connected assets
	Data breaches
	Identity theft
	Exploitation of software bugs
	Abuse of authorisation
	Abuse of information leakages
	Intentional disclosure
	Falsification of records including certification
	Eavesdropping and/or wiretapping
Type	**Insider threats**
	Stealing information or manipulation of data
	Sales of important data to competitors
	Leaking information
Type	**Unintentional damage**
	Operator and/or user errors
	Configuration errors
	Accidental disclosure
	Mismanagement

Table 2 Results of first iteration during applying our methodology on the HR system.

Step	Results
System modeling	Problem frames: "PF1: Salary Info editing" Requirement: *Salary info is edited by users* "PF2: Salary Info display" Requirement: *Salary information is displayed to users*
Identify assets	Assets: Salary Information
Identify threats and vulnerabilities	Abuse frames diagrams: "AF1: Information disclosure of salary information" AR: *Salary information is displayed to attackers without authorization* "AF2: Tampering Salary information" AR: *Attacker makes modifications to salary information without authorization*
Identify security requirements	"SPF1: Integrity preserving of salary information" SR: *Modification or creation of salary information is allowed only to authorized HR staff and not allowed to unauthorized users* "SPF2: Confidentiality preserving of salary information" SR: *Authorized HR staff only is allowed to view salary information*
Security requirements evaluation	The requirements complete each other and do not cause conflicts

Gambar II.4: Contoh Penggunaan Metodologi Security Requirement Elicitation *[2]*

3. *Threats and vulnerabilities identification*
4. *Security requirements elicitation*
5. *Security requirements evaluation*

Contoh penggunaan metodologi ini dapat dilihat pada Gambar 2.4.

II.5 STRIDE *Threat List*

Untuk mendukung metodologi *Security Requirement Elicitation*, maka digunakan kategori STRIDE. Jenis ancaman dari kategori STRIDE dapat dilihat pada Tabel 2.3.

Tabel II.3: STRIDE Threat List [4]

Type	Examples	Security Control
Spoofing	Ancaman yang bertujuan untuk mengakses dan menggunakan credential orang lain secara ilegal	Authentication
Tampering	Ancaman yang bertujuan untuk mengubah data tetap, seperti data pada database, dan perubahan data pada transit antar dua komputer pada jaringan terbuka seperti internet	Integrity
Repudiation	Ancaman yang bertujuan untuk melakukan operasi ilegal pada sistem yang lemah dalam hal melacak operasi terlarang	Non-repudiation
Information Disclosure	Ancaman untuk membaca sebuah file yang tidak diperbolehkan untuk diakses, atau membaca data in transit	Confidentiality
Denial of Service	Ancaman yang bertujuan untuk menolak akses pada user yang valid dengan membuat web server tidak dapat digunakan sementara	Availability
Elevation of Privilege	Ancaman yang bertujuan untuk mendapatkan hak akses kepada sumber daya untuk mendapatkan akses yang tidak berwenang pada informasi atau untuk mengkompromi sistem	Authorization

Bab III

Stakeholder Requirement dan *System Requirement*

Pada penelitian ini, dari 11 proses NIST SP 800-160, proses yang akan dilakukan adalah *stakeholder requirement definition process* dan *requirement analysis process*. Setelah didapatkan *stakeholder requirement*, maka akan diturunkan menjadi *system requirement*. Tabel 3.1 berikut ini menjabarkan *stakeholder requirement* untuk Sistem Pembayaran Elektronik Angkutan Kota berdasarkan analisis dari kebutuhan pada penelitian sebelumnya. Kemudian dari *stakeholder requirement* tersebut diturunkan menjadi *system requirement* seperti pada Tabel 3.2. *System requirement* ini digunakan sebagai *problem frames* untuk proses *security requirement elicitation*.

Tabel III.1: *Stakeholder Requirement* Sistem Pembayaran Elektronik Angkutan Kota

Stakeholder terkait	ID	*Requirement*
Penumpang (passenger)	SR-P-01	Mendapatkan tarif yang fair, setiap angkot sama untuk jarak tempuh yang sama
	SR-P-02	Transaksi yang cepat
	SR-P-03	Transaksi yang aman
	SR-P-04	Transaksi dapat dilakukan di semua angkot Kota Bandung
	SR-P-05	Transaksi dapat dilakukan setiap saat menaiki angkot
	SR-P-06	Penumpang dapat membayarkan tarif angkot untuk lebih dari 1 penumpang
	SR-P-07	Mengetahui ketersediaan saldo
	SR-P-08	Dapat mengisi saldo kartu (top up)
	SR-P-09	Mengetahui pemindaian kartu berhasil atau tidak
	SR-P-10	Transaksi hanya dapat dilakukan pada 1 kendaraan di waktu bersamaan oleh ID yang sama (single sign on)
Supir (Driver)	SR-D-01	Mendapatkan tarif angkot sesuai jarak tempuh penumpang
	SR-D-02	Mengetahui akumulasi pendapatan setiap hari
	SR-D-03	Mengetahui pemindaian kartu penumpang telah dilakukan atau belum
Pemilik/Pengelola (Owner)	SR-O-01	Mendapatkan hasil setoran dari supir
	SR-O-02	Mengetahui pendapatan supir angkot
	SR-O-03	Memastikan bahwa tidak ada kecurangan yang dilakukan penumpang atau supir
	SR-O-04	Memberikan pelayanan yang baik agar masyarakat mau menggunakan angkot
	SR-O-05	Memastikan supir tertib lalu lintas (dalam trayek)

Tabel III.2: System Requirement

No.	System Requirement
1	Sistem dapat menghitung tarif untuk setiap penumpang
2	Sistem dapat menampilkan tarif penumpang
3	Sistem dapat memotong saldo penumpang
4	Sistem dapat mengidentifikasi penumpang naik dan turun
5	Sistem dapat mengidentifikasi user yang membuka log transaksi (supir atau pengelola)
6	Sistem tidak boleh mengizinkan penumpang untuk melakukan transaksi beberapa kali dalam 1 sesi (single sign on)
7	Sistem harus dapat mengetahui pengiriman data berasal dari mana, apakah benar dari device pada angkot atau akses langsung dari browser (tidak boleh)
8	Sistem harus dapat membedakan hak akses user, sehingga akses data credential hanya dapat dilakukan oleh sysadmin
9	Sistem dapat membedakan device yang ada pada setiap angkot, sehingga integritas data dapat terpenuhi
10	Sistem memiliki availability yang tinggi
11	Sistem menyediakan pilihan untuk jumlah penumpang yang akan dibayarkan oleh user saat naik
12	Sistem menampilkan sisa saldo penumpang saat penumpang melakukan scan kartu naik maupun turun
13	Sistem memberikan feedback saat penumpang memindai kartu naik dan turun
14	Sistem dapat menghitung akumulasi pendapatan setiap supir
15	Sistem memungkinkan user supir untuk melihat akumulasi pendapatan
16	Sistem dapat mengidentifikasi setiap supir
17	Sistem memungkinkan supir untuk mengetahui pemindaian kartu oleh penumpang
18	Sistem melakukan penambahan tarif penumpang setiap angkot melewati area checkpoint

Bab IV

Security Requirement

Berdasarkan metodologi *Security Requirement Elicitation*, terdapat 5 langkah untuk mendapatkan *security requirement* antara lain:

1. *System modeling*
2. *Assets identification*
3. *Threats and vulnerabilities identification*
4. *Security requirements elicitation*
5. *Security requirements evaluation*

Pada penelitian ini, *problem frames* (PF) yang digunakan berasal dari *system requirement* yang diturunkan dari *stakeholder requirement. Abuse frames* (AF) yang digunakan adalah dengan menggunakan kategori STRIDE. Sebagian dari ancaman *intelligent public transport* (IPT) tercakup dalam STRIDE, sehingga digunakan STRIDE sebagai *abuse frames* pada iterasi ini.

Proses yang dilakukan berdasarkan metodologi *Security Requirement Elicitation* dibagi menjadi 3 bagian yang dikelompokkan berdasarkan aset, yaitu aset data transaksi, aset data penumpang, dan aset data supir. Hasil dari penggunaan metodologi untuk aset data transaksi dapat dilihat pada Tabel 4.1, aset data penumpang yang dapat dilihat pada Tabel 4.2, dan aset data supir yang dapat dilihat pada Tabel 4.3. Dari proses tersebut dihasilkan 14 poin *security requirement* yang dapat dilihat pada Tabel 4.4.

Tabel IV.1: Hasil dari Penggunaan Metodologi untuk *Security Requirement Elicitation* untuk Aset Data Transaksi

Steps	Result	
System Modeling	PF1:	Sistem dapat menghitung tarif untuk setiap penumpang
	Requirement	Tarif dihitung secara otomatis untuk setiap penumpang
	PF2:	Sistem dapat menampilkan tarif penumpang
	Requirement	Tarif ditampilkan kepada penumpang dan supir
	PF3:	Sistem melakukan penambahan tarif penumpang setiap angkot melewati area checkpoint
	Requirement	Tarif penumpang yang ada di dalam angkot bertambah saat melewati area checkpoint
	PF4:	Sistem dapat mengidentifikasi user yang membuka log transaksi (supir atau pengelola)
	Requirement	Log transaksi dapat dilihat oleh user supir dan pengelola
Identify Assets	Aset:	Data transaksi (Id penumpang dan tarif), log transaksi, data angkot (id angkot dan lokasi)
Identify threats and vulnerabilities	AF1:	Keterbukaan informasi data transaksi
	AR	Data transaksi diketahui attacker
	AF2:	Tampering data transaksi
	AR	Attacker melakukan modifikasi tarif penumpang
	AF3:	Denial of Service pada transaksi
	AR	Attacker membuat transaksi tidak berhasil dilakukan
	AF4:	Tampering data angkot
	AR	Attacker melakukan modifikasi lokasi angkot
	AF5:	Elevation of Privilege sebagai system administrator
	AR	Attacker memiliki hak akses sebagai system administrator
Identify Security Requirement	SPF1:	Confidentiality preserving pada data transaksi
	SR	Data transaksi (Log transaksi) hanya dapat diakses oleh supir dan pengelola yang terautorisasi
	SPF2:	Integrity preserving pada data transaksi
	SR	Data transaksi (log transaksi) tidak dapat dimodifikasi dan data transaksi hanya dapat dibuat saat penumpang melakukan transaksi (memindai kartu saat naik angkot)
	SPF3:	Availability pada proses transaksi
	SR	Mencegah dan menangani DoS dengan mendeteksi adanya DoS pada sistem
	SRF4:	Integrity preserving pada data angkot
	SR	Data lokasi angkot hanya dapat diupdate saat angkot melewati lokasi checkpoint, tidak dapat dimodifikasi kecuali oleh system admin
	SRF5:	Authorization preserving
	SR	Hak akses harus dibedakan untuk tiap user dan harus dilakukan autorisasi untuk membedakan tiap user
Security Requirement Evaluation		Requirement memenuhi satu sama lain dan tidak konflik

Tabel IV.2: Hasil dari Penggunaan Metodologi untuk Security Requirement Elicitation untuk Aset Data Penumpang

Steps	Result	
System Modeling	PF5:	Sistem dapat mengidentifikasi penumpang naik dan turun
	Requirement	Penumpang dapat teridentifikasi saat naik dan turun angkot dan dapat melakukan transaksi
	PF6:	Sistem dapat memotong saldo penumpang
	Requirement	Saldo penumpang terpotong secara otomatis saat turun sesuai dengan tarif yang dihitung
	PF7:	Sistem menampilkan sisa saldo penumpang saat penumpang melakukan scan kartu naik maupun turun
	Requirement	Saldo penumpang ditampilkan kepada penumpang saat akan melakukan pemindaian kartu
	PF8:	Single sign on
	Requirement	Transaksi oleh 1 user hanya dapat dilakukan pada 1 angkot dalam 1 waktu
Identify Assets	Aset:	Data penumpang (ID dan saldo) dan data transaksi (ID dan tarif)
Identify threats and vulnerabilities	AF6:	Spoofing sebuah transaksi
	AR	Attacker menipu sebuah transaksi dengan mengakses langsung web server dan melakukan transaksi dengan data penumpang lain
	AF7:	Tampering saldo penumpang
	AR	Attacker mengubah saldo penumpang
	AF8:	Keterbukaan informasi data penumpang pada saat melakukan transaksi
	AR	Attacker mengetahui data penumpang dan dapat menggunakannya untuk transaksi dengan mengakses langsung web sever
	AF9:	Repudiation pada transaksi yang berlangsung
	AR	Attacker dapat mengakses langsung web server dan memanipulasi transaksi tanpa terlacak
	AF10:	Denial of Service pada transaksi
	AR	Attacker membuat transaksi yang legitimate gagal dengan melakukan transaksi palsu sehingga sistem hanya memroses transaksi yang dilakukan oleh attacker
	AF11:	Tampering data transaksi pada angkot berbeda
	AR	Attacker melakukan transaksi dengan data penumpang yang sama pada 2 angkot berbeda
Identify Security Requirement	SPF6:	Authentication pada saat transaksi berlangsung
	SR	Sistem dapat mendeteksi user yang legitimate saat melakukan transaksi
	SRF7:	Integrity pada data saldo penumpang
	SR	Saldo penumpang hanya dapat dimodifikasi oleh sistem secara otomatis saat penumpang turun dan saat penumpang melakukan top-up
	SRF8:	Confidentiality data penumpang
	SR	Data penumpang dan data transaksi tidak boleh terbaca jelas saat in transit (harus terenkripsi)
	SRF9:	Non-repudation pada transaksi yang berlangsung
	SR	Setiap transaksi harus dapat terlacak asalnya (dari device pada angkot atau akses langsung web server) dan tersimpan pada log
	SRF10:	Availability pada transaksi
	SR	Transaksi yang bukan berasal dari device pada angkot harus ditolak sehingga tidak mengganggu avalability dari sistem yang seharusnya
	SRF11:	Integrity preserving pada data transaksi
	SR	Sistem dapat membedakan setiap device pada angkot sehingga menjamin integritas data transaksi
Security Requirement Evaluation		Requirement memenuhi satu sama lain dan tidak konflik

Tabel IV.3: Hasil dari Penggunaan Metodologi untuk Security Requirement Elicitation untuk Aset Data Supir

Steps	Result	
System Modeling	PF9:	Sistem dapat mengidentifikasi setiap supir
	Requirement	Supir dapat teridentifikasi saat melihat log dan akumulasi pendapatan
	PF10:	Sistem dapat menghitung akumulasi pendapatan setiap supir
	Requirement	Akumulasi pendapatan dihitung dari penjumlahan tarif penumpang pada angkot yang bersangkutan
	PF11:	Sistem memungkinkan user supir untuk melihat akumulasi pendapatan
	Requirement	Akumulasi pendapatan dapat dilihat oleh supir yang bersangkutan
	PF12:	Sistem memungkinkan supir untuk mengetahui pemindaian kartu oleh penumpang
	Requirement	Pemindaian kartu yang berhasil memberikan feedback sehingga dapat diketahui oleh supir dan penumpang jika pemindaian berhasil dilakukan
Identify Assets	Aset:	Data supir
Identify threats and vulnerabilities	AF12:	Tampering data pendapatan supir
	AR	Attacker memanipulasi hasil pendapatan supir
	AF13:	Information Disclosure pendapatan supir
	AR	Attacker melihat hasil pendapatan supir
	AF14:	Tampering feedback pemindaian kartu
	AR	Attacker memanipulasi feedback pemindaian kartu sehingga transaksi terjadi berulang
Identify Security Requirement	SPF12:	Integrity preserving data pendapatan supir
	SR	Akumulasi pendapatan supir tidak dapat dimodifikasi, hanya akan bertambah setiap ada transaksi di angkot yang bersangkutan
	SRF13:	Confidentiality preserving data pendapatan supir
	SR	Akumulasi pendapatan supir tidak dapat dilihat kecuali oleh supir yang terautentikasi dan tidak boleh terbaca saat data in transit
	SRF14:	Integrity preserving feedback pemindaian kartu
	SR	Pengecekan terhadap transaksi yang janggal (pemindaian dalam waktu yang terlalu dekat berkali-kali)
Security Requirement Evaluation		Requirement memenuhi satu sama lain dan tidak konflik

Tabel IV.4: Security Requirement

ID	Security Requirement Sistem Pembayaran Elektronik Angkutan Kota
SR1	Data transaksi (Log transaksi) hanya dapat diakses oleh supir dan pengelola yang terautorisasi
SR2	Data transaksi (log transaksi) tidak dapat dimodifikasi dan data transaksi hanya dapat dibuat saat penumpang melakukan transaksi (memindai kartu saat naik angkot)
SR3	Mencegah dan menangani DoS dengan mendeteksi adanya DoS pada sistem
SR4	Data lokasi angkot hanya dapat diupdate saat angkot melewati lokasi checkpoint, tidak dapat dimodifikasi kecuali oleh system admin
SR5	Hak akses harus dibedakan untuk tiap user dan harus dilakukan autorisasi untuk membedakan tiap user
SR6	Sistem dapat mendeteksi user yang legitimate saat melakukan transaksi
SR7	Saldo penumpang hanya dapat dimodifikasi oleh sistem secara otomatis saat penumpang turun dan saat penumpang melakukan top-up
SR8	Data penumpang dan data transaksi tidak boleh terbaca jelas saat in transit (harus terenkripsi)
SR9	Setiap transaksi harus dapat terlacak asalnya (dari device pada angkot atau akses langsung web server) dan tersimpan pada log
SR10	Transaksi yang bukan berasal dari device pada angkot harus ditolak sehingga tidak mengganggu avalability dari sistem yang seharusnya
SR11	Sistem dapat membedakan setiap device pada angkot sehingga menjamin integritas data transaksi
SR12	Akumulasi pendapatan supir tidak dapat dimodifikasi, hanya akan bertambah setiap ada transaksi di angkot yang bersangkutan
SR13	Akumulasi pendapatan supir tidak dapat dilihat kecuali oleh supir yang terautentikasi dan tidak boleh terbaca saat data in transit
SR14	Pengecekan terhadap transaksi yang janggal (pemindaian dalam waktu yang terlalu dekat berkali-kali)

Bab V

Simpulan dan Saran

V.1 Simpulan

Metodologi untuk *security requirement elicitation* yang digunakan terdiri dari 5 langkah yaitu *system modeling*, *asset identification*, *threats and vulnerabilities identification*, *security requirement elicitation*, dan *security requirement evaluation*. *Problem frames* pada *system modeling* menggunakan *system requirement* yang diturunkan dari *stakeholder requirement*. Dari identifikasi dan analisis yang dilakukan, dihasilkan 14 *security requirement* untuk Sistem Pembayaran Elektronik Angkutan Kota.

V.2 Saran

Pada makalah ini masih terdapat banyak kekurangan, seperti iterasi metodologi yang hanya dilakukan satu kali dan identifikasi ancaman yang masih dapat digali lebih dalam lagi. Untuk penelitian selanjutnya, dapat dilakukan analisis yang lebih dalam untuk menghasilkan *security requirement* yang lebih lengkap. Penelitian selanjutnya dapat menggunakan *threat modeling* yang lebih lengkap dan/atau melakukan *security requirement elicitation* lebih dari satu kali iterasi sehingga *security requirement* yang dihasilkan lebih spesifik dan lengkap.

Bibliografi

[1] K. Ummah and K. Mutijarsa, "Design and development prototype of electronic payment system for angkot case study: City of bandung, indonesia", in *2015 International Conference on Information Technology Systems and Innovation (ICITSI)*, Nov 2015, pp. 1–6.

[2] Hassan El-Hadary and Sherif El-Kassas, "Capturing security requirements for software systems", *Journal of Advanced Research*, vol. 5, no. 4, pp. 463–472, 2014.

[3] European Union Agency For Network Security and Information, *Cyber Security and Resilience of Intelligent Public Transport Good practices and recommendations*, Number December. 2015.

[4] Marco M. Morana, "Managing Software Security Risks Using Application Threat Modeling", 2008.

[5] Ron Ross, Janet Carrier Oren, and Michael McEvilley, "NIST Special Publication 800-160: Systems Security Engineering", Tech. Rep., National Institute of Standards and Technology, 2014.