

DAFTAR ISI

HALAMAN JUDUL	i
PERNYATAAN BEBAS PLAGIARISME	ii
KATA PENGANTAR.....	vi
DAFTAR TABEL	x
DAFTAR GAMBAR.....	xi
DAFTAR LAMBANG DAN SINGKATAN.....	xiii
INTISARI.....	xiv
ABSTRACT	xv
BAB I PENDAHULUAN	1
I.1. Latar Belakang.....	1
I.2. Perumusan Masalah.....	2
I.2.1. Batasan Masalah.....	2
I.3. Tujuan Penelitian.....	3
I.4. Manfaat Penelitian.....	3
BAB II TINJAUAN PUSTAKA.....	4
BAB III DASAR TEORI	7
III.1. <i>Industrial Control System (ICS)</i>	7
III.2. Protokol Komunikasi S7CommPlus	8
III.3. Serangan <i>Man-in-the-Middle (MitM)</i>	9
III.4. Metrik Performa Komunikasi Jaringan.....	11
BAB IV PELAKSANAAN PENELITIAN.....	14
IV.1. Alat dan Bahan Penelitian	14
IV.2. Tata Laksana Penelitian.....	16
IV.2.1. Analisis Jaringan dan Kerentanan ICS <i>Testbed</i>	17
IV.2.2. Perancangan dan Implementasi Serangan MitM.....	18
IV.2.3. Evaluasi Dampak Serangan MitM.....	20
IV.3. Rencana Analisis Hasil Penelitian	21
BAB V HASIL DAN PEMBAHASAN.....	23
V.1. Hasil Analisis Jaringan dan Kerentanan ICS <i>Testbed</i>	23



V.2. Hasil Perancangan dan Implementasi Serangan MitM	27
V.3. Hasil Evaluasi Dampak Serangan MitM.....	29
V.4. Hasil Analisis Statistik Deskriptif	34
BAB VI KESIMPULAN DAN SARAN	39
VI.1. Kesimpulan.....	39
VI.2. Saran.....	39
DAFTAR PUSTAKA.....	40

DAFTAR TABEL

Tabel 2.1. Posisi penelitian dan penelitian terdahulu.	6
Tabel 4.1. Perangkat keras penelitian.	14
Tabel 4.2. Perangkat lunak penelitian.	15
Tabel 4.3. Target serangan yang akan dimanipulas pada alamat memori PLC.....	19
Tabel 5.1. Pengukuran statistik skenario pertama	34
Tabel 5.2. Pengukuran statistik skenario kedua	36

DAFTAR GAMBAR

Gambar 3.1. Operasi ICS.....	7
Gambar 3.2. Arsitektur protokol S7CommPlus.....	8
Gambar 3.3. Struktur protokol S7CommPlus.....	9
Gambar 3.4. Posisi penyerang.	10
Gambar 3.5. Pengukuran <i>Round-Trip Time</i> (RTT).	12
Gambar 4.1. ICS <i>Testbed</i>	16
Gambar 4.2. Diagram alir tata laksana penelitian	17
Gambar 4.3. Filter paket Ettercap.....	18
Gambar 4.4. Rancangan skenario serangan.....	19
Gambar 4.5. Proses pengukuran performa komunikasi.....	21
Gambar 5.1. Hasil pemindaian Netdiscover	23
Gambar 5.2. Hasil tangkapan Wireshark.....	23
Gambar 5.3. Topologi jaringan ICS <i>Testbed</i>	24
Gambar 5.4. Analisis <i>payload</i> paket.....	24
Gambar 5.5. Analisis <i>subscription</i> data.....	25
Gambar 5.6. Proses komunikasi PLC dan <i>Engineering Workstation</i>	26
Gambar 5.7. Paket kunci sesi komunikasi.....	26
Gambar 5.8. Tampilan log Ettercap.	27
Gambar 5.9. <i>Engineering Workstation</i> kehilangan koneksi.....	28
Gambar 5.10. Log eksekusi injeksi data palsu.	28
Gambar 5.11. <i>Engineering Workstation</i> menampilkan data palsu.	29
Gambar 5.12. Tanda awal sebelum serangan terjadi.....	30
Gambar 5.13. Tampilan <i>trend</i> nilai proses saat terjadi serangan.....	30
Gambar 5.14. PLC mengakhiri sesi dengan <i>Engineering Workstation</i>	31
Gambar 5.15. Grafik pengukuran RTT skenario pertama.....	31
Gambar 5.16. Grafik pengukuran <i>Throughput</i> skenario pertama.....	32
Gambar 5.17. Grafik pengukuran RTT skenario kedua	33
Gambar 5.18. Grafik pengukuran <i>Throughput</i> skenario kedua.....	33

Gambar 5.19. Boxplot distribusi nilai RTT skenario pertama	35
Gambar 5.20. Boxplot distribusi nilai <i>Throughput</i> skenario pertama.	36
Gambar 5.21. Boxplot distribusi nilai RTT skenario kedua.....	37
Gambar 5.22. Boxplot distribusi nilai <i>Throughput</i> skenario kedua	38