UNIVERSITÄT
DUISBURG
ESSEN

A Distributed Infrastructure to Analyse SIP Attacks in Internet using the NorNet Testbed

UNIVERSITÄT
DUISBURG
ESSEN

Adnan Aziz
Networking Technology Group
Institute for Experimental Mathematics &
Institute for Computer Science & Business
Information Systems
University of Duisburg-Essen

Overview

- Introduction
  - SIP-based VoIP threats
  - SIP-based multi-stage Toll Fraud
- Related Work
  - HoneyNet System and STR
  - Monitoring Sensors
- NorNet Central Sensor Approach
  - Motivation
  - Architecture
  - Results
- Conclusions

SIP-based VoIP Threats

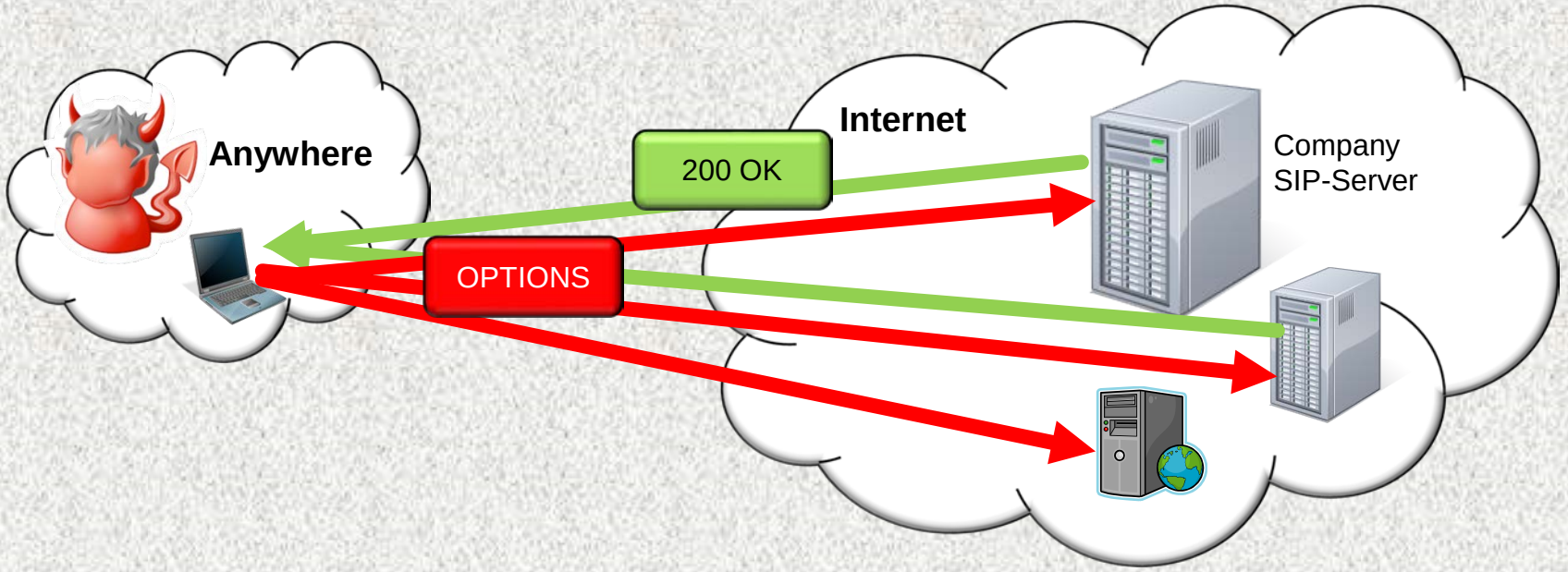
- Signaling communication protocol
- SIP has appeared as a de facto standard for VoIP
- Attack tools are readily available and are already in use
  - SIPvicious [1]
  - Analysis of a “/0” Stealth Scan from a Botnet [2]
    - Flooding
    - Fuzzing
    - SPITING
    - **Toll Fraud**
- Toll Fraud provides immediate financial benefits
  - Call to premium numbers
  - International calls

- **We are analyzing this attack traffic since 2009.**
- **Captured more than 150 million SIP packets**

[1] http://blog.SIPVicious.org
[2] Alberto Dainotti, Alistair King, kc Claffy, Ferdinando Papale, Antonio Pescapé, Analysis of a “/0” Stealth Scan from a Botnet, proceedings of ACM SIGCOMM Internet Measurement Conference 2012.

Multi Stage Toll Fraud

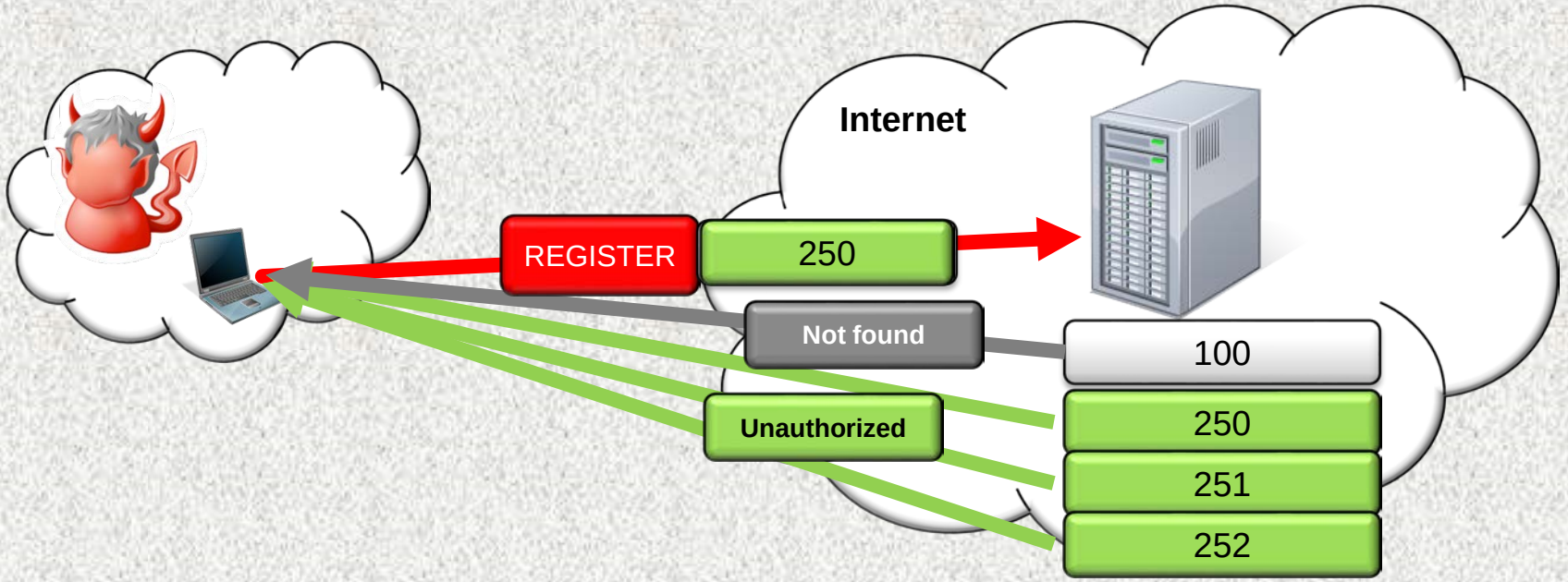
Stage 1: Server Scan



- List of active SIP servers

Multi Stage Toll Fraud

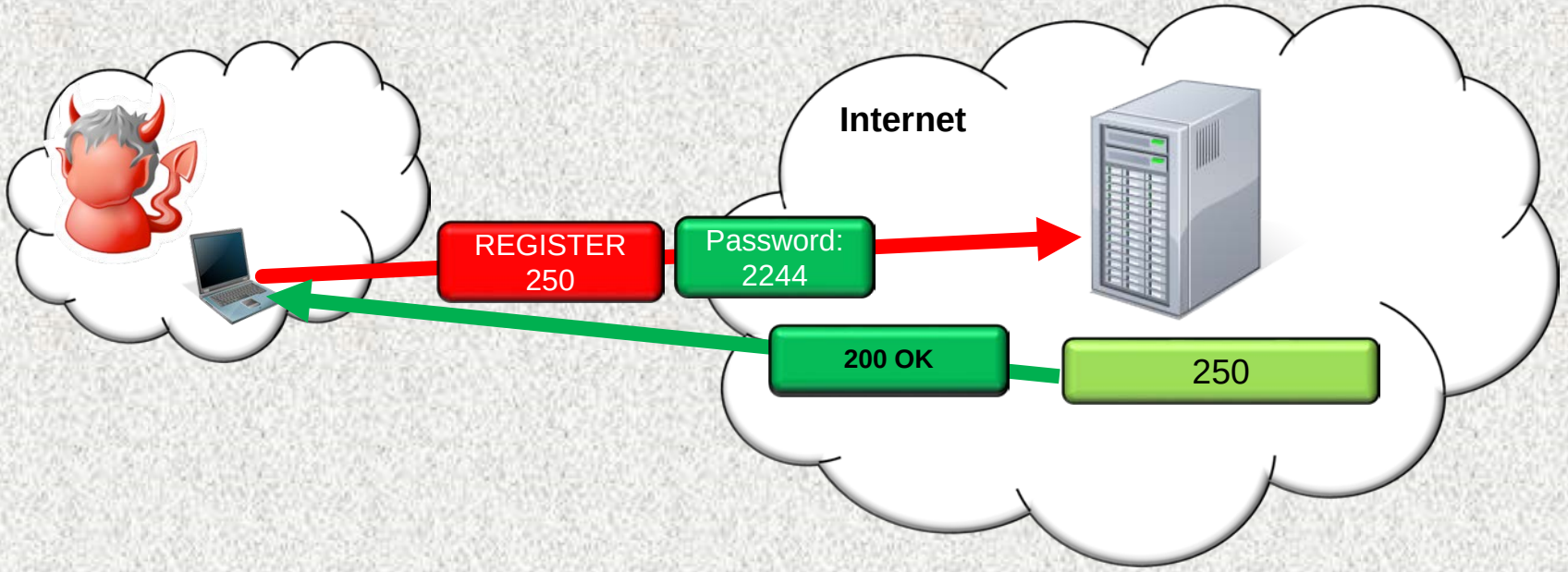
Stage 2: Extension Scan



- List of active SIP servers
- List of active extensions/user accounts

Multi Stage Toll Fraud

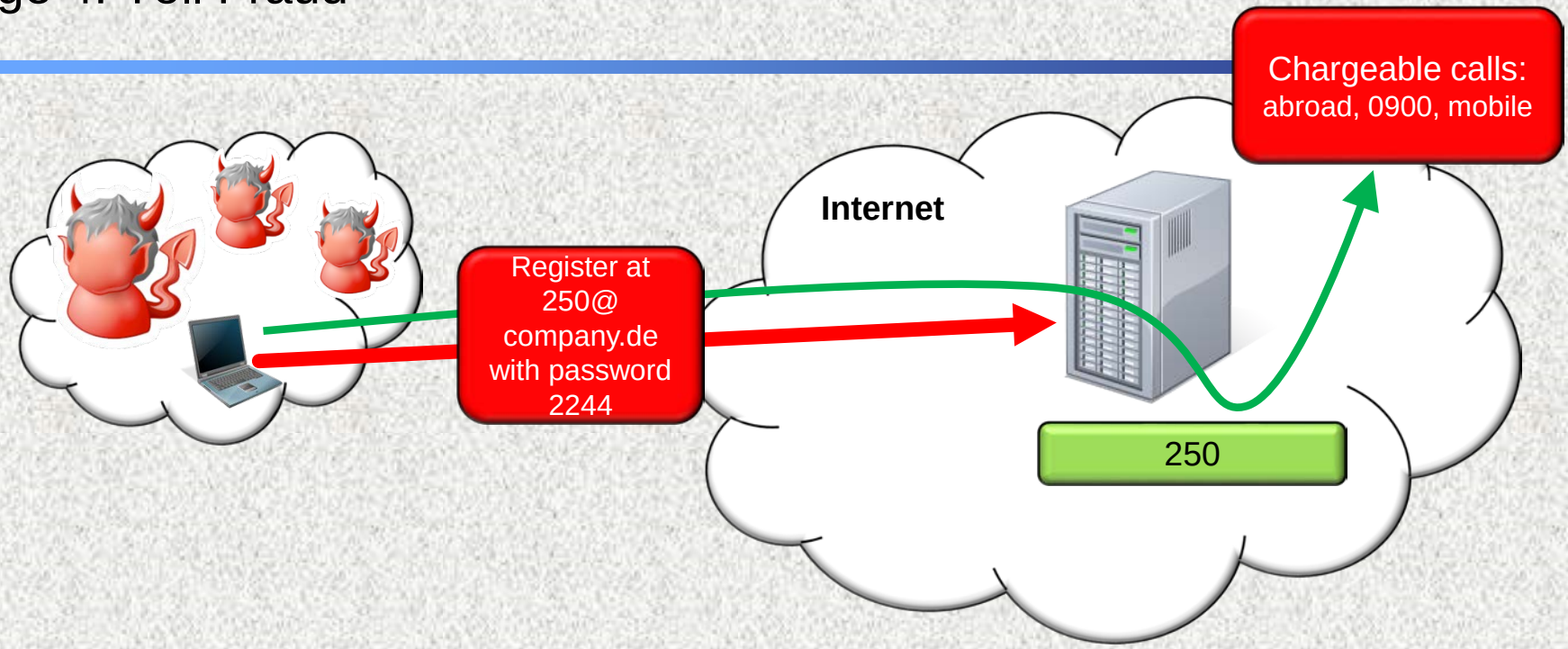
Stage 3: Registration Hijacking



- List of active SIP servers
- List of active extensions/user accounts
- Valid credentials for active extension

Multi Stage Toll Fraud

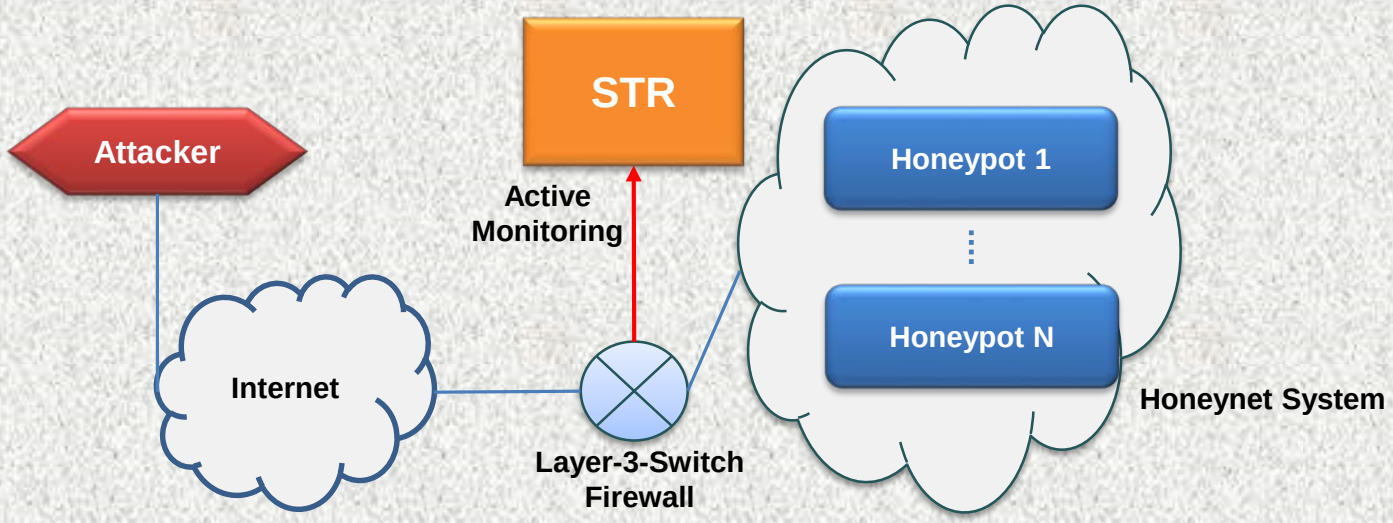
Stage 4: Toll Fraud



- List of active SIP servers
- List of active extensions/user accounts
- Valid credentials for active extension
- Calls via victim‘s account

Related Work

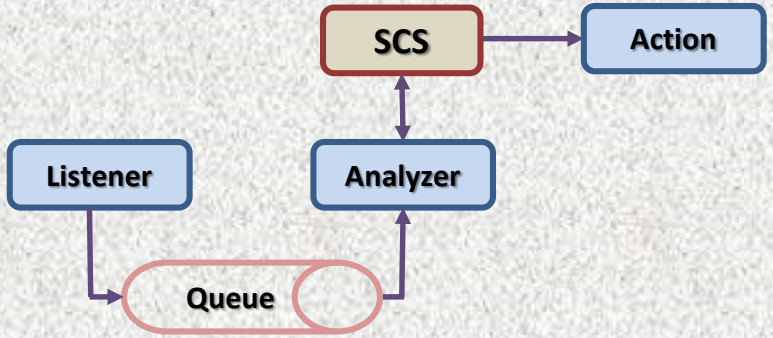
Honeynet System and SIP Trace Recorder



- VoIP Honeypots
  - Standard Linux Virtual Machine
    - Open source VoIP PBX Asterisk server
    - Dionaea Honeypot
  - Acts as SIP server
    - Accepts incoming requests
    - Respond to these requests
- SIP Trace Recorder (STR)
  - Traces & logs all SIP requests and responses
    - Parses & analyze header values
    - Store in database
  - Automatically generates Reports
    - SIP packets per day
    - Clustering SIP packets by attack stages

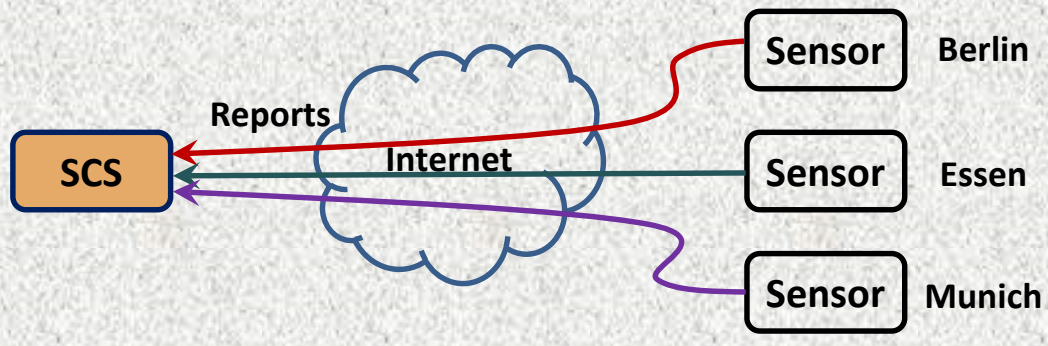
Related Work
Monitoring Sensors

- Sensors
  - Light-weight software component for different hardware software platform
    - Implemented in C++ and Java
  - Rule based
  - Misuse detection and reporting
    - Real-time



- Sensor Central Service (SCS)
  - Maintenance and attack correlation

Related Work
Distributed Approach



- Deployment of hardware or installation of software required
- Local management necessary
- Privileged access to network interfaces required

NorNet Central Sensor Approach
Motivation

UNIVERSITÄT DUISBURG ESSEN

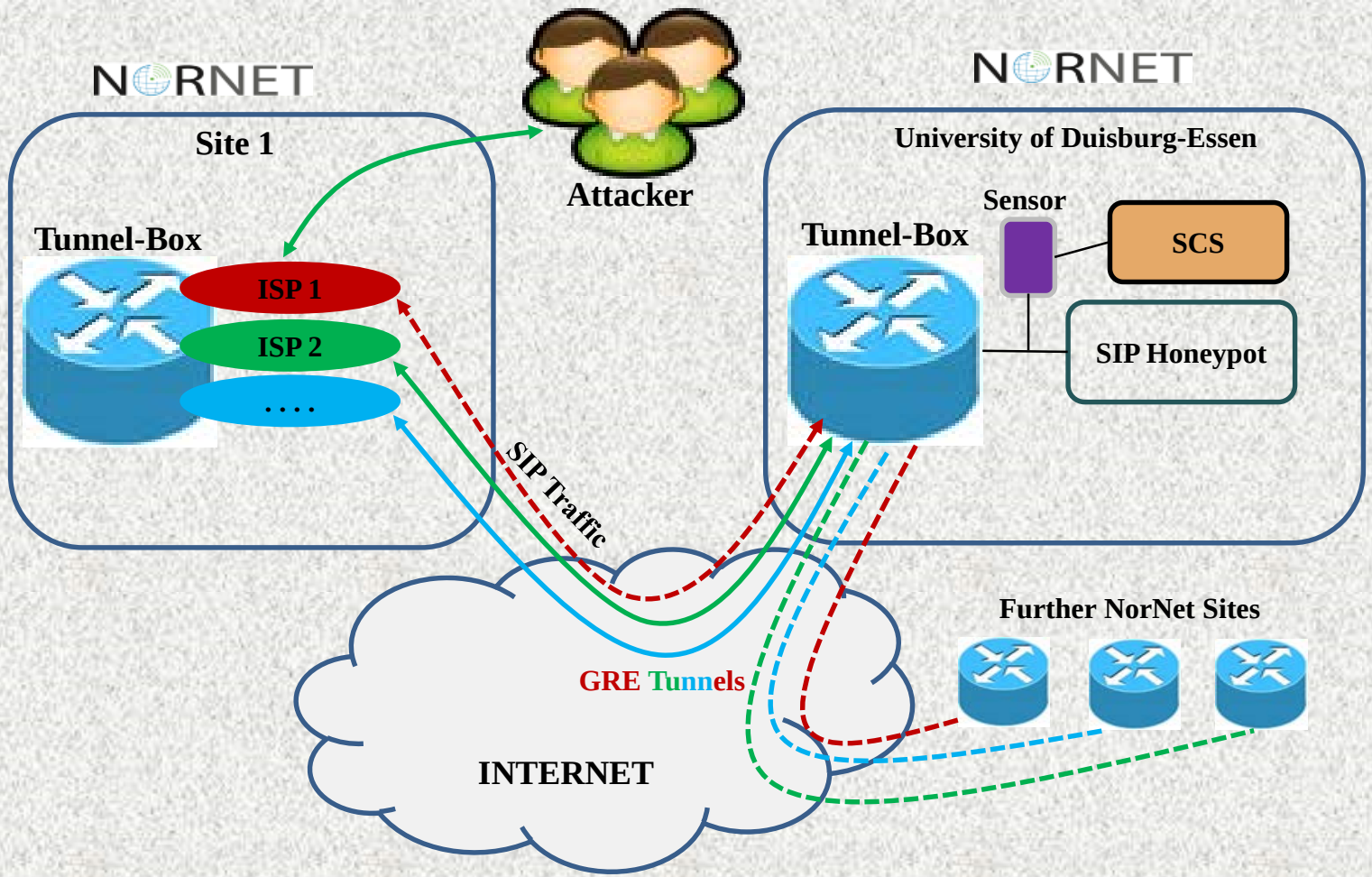
- Sensor Deployment requires
  - Configuration, Maintenance and Updating of Hardware and Software
- NorNet
  - Distributed all over Norway and some International locations
  - Consists of
    - 3G wireless (NorNet Edge)
    - Wired part (NorNet Core)
  - Multi-homed
  - Rule-based Routing

NorNet Central Sensor Approach

UNIVERSITÄT DUISBURG ESSEN

- One central Sensor only (in Essen, Germany)
  - No hardware and software installation in NorNet
- Distributed NorNet nodes to capture input traffic
  - GRE Tunnel(s) between each node and the central site
  - Filters TCP/UDP traffic on port 5060
  - Traffic redirection to the central Sensor by using DNAT via GRE tunnels
  - Reverse direction is realized by routing policies
- Pros
  - No additional software component in NorNet system
  - Easy to manage single sensor
  - Easy installation in other productive environments (no influence)
- Cons
  - More bandwidth required in contrast to distributed approach
  - Possible delays

NorNet Architecture



Attack Statistics

UNIVERSITÄT DUISBURG ESSEN

Data taken from October 15 2013 to August 15 , 2014.

External IP	Internal IP	Nodes	# of attackers	SS	ES	RHJ	INVITE
158.39.4.2	172.31.1.1	Simula 1	792	572	50	14657	180
77.88.71.151	172.31.1.2	Simula 2	1847	1360	223	129	374
62.92.88.42	172.31.1.3	Simula 3	390	342	0	0	7
158.39.93.231	172.31.10.1	Hogskolen i Narvik 1	770	564	48	128	169
195.159.158.174	172.31.10.2	Hogskolen i Narvik 2	599	482	11	11	83
129.240.66.74	172.31.2.1	Universitetet i Oslo 1	595	494	15	2251	72
195.159.158.198	172.31.2.2	Universitetet i Oslo 2	530	473	0	0	21
85.252.121.218	172.31.2.3	Universitetet i Oslo 3	480	443	0	0	14
128.39.49.154	172.31.3.1	HIG 1	445	379	5	55	37
95.159.158.254	172.31.3.2	HIG 2	536	484	0	0	20
193.10.227.85	172.31.30.1	KAU 1	618	518	8	9	73
129.242.157.228	172.31.4.1	Universitetet i Tromso 1	851	615	61	127	185
195.159.158.162	172.31.4.2	Universitetet i Tromso 2	534	479	0	0	21
62.92.89.210	172.31.4.3	Universitetet i Tromso 3	479	435	0	0	8
132.252.152.105	172.31.42.1	DUE 1	842	605	73	281	189
89.246.242.228	172.31.42.2	DUE 2	1341	1062	122	177	223
152.94.120.6	172.31.5.1	Universitetet i Stavanger 1	777	554	44	50	172
195.159.158.210	172.31.5.2	Universitetet i Stavanger 2	534	479	0	0	20
158.37.6.195	172.31.6.1	Universitetet i Bergen 1	769	556	45	256	169
62.97.202.70 5	172.31.6.2	Universitetet i Bergen 2	1245	1066	40	362	128
158.36.50.178	172.31.7.1	Universitetet i Agder 1	803	575	52	500	176
195.159.203.50	172.31.7.2	Universitetet i Agder 2	533	476	0	0	23
158.39.149.13	172.31.8.1	Universitetet pa Svalbard 1	773	561	47	231	174
210.37.45.149	172.31.88.1	Hainan University 1	982	876	21	193	89
113.59.104.58	172.31.88.2	Hainan University 2	718	700	0	0	10
129.241.200.128	172.31.9.1	NTNU Trondheim 1	866	626	70	205	183
195.159.158.134	172.31.9.2	NTNU Trondheim 2	533	476	0	0	21

Attack Distribution

- Most of attackers attacked single nodes
- Some attackers attacked most/all nodes
- Not in close proximity
  - With respect to IP addresses (113.0.0.0 – 89.0.0.0) and physical location (Different Continents)
  - Large IP range is scanned
- Evaluated attacks from same source IP with respect to time
  - Nodes in close proximity took few minutes to an hour to scan IP range
  - One week to a month to scan whole IP range (Germany, Norway and China)

# of Nodes	# of Attackers	# of Nodes	# of Attackers
1	1712	15	78
2	615	16	39
3	358	17	21
4	237	18	18
5	159	19	15
6	117	20	23
7	108	21	25
8	105	22	30
9	130	23	26
10	106	24	26
11	84	25	30
12	87	26	40
13	78	27	34
14	73	28	10

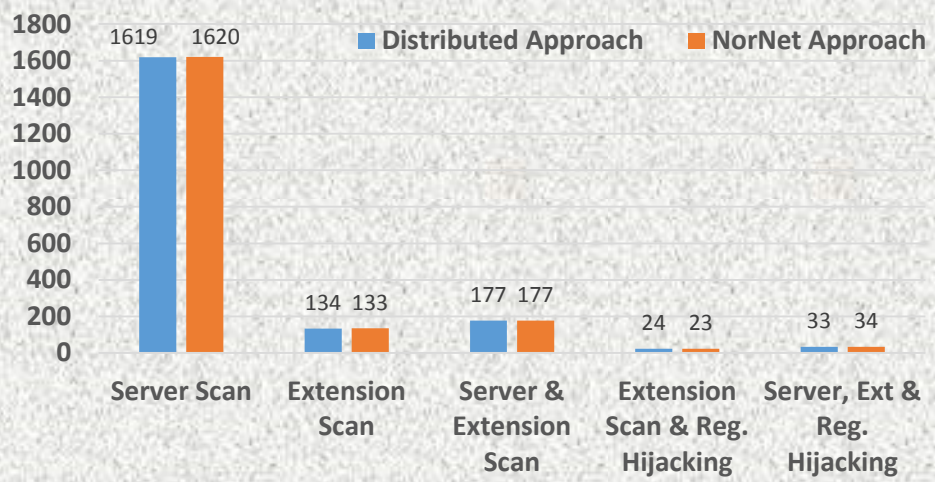
Attacker Behavior

	N12	N19	N14	N13	N4	N5	N7	N9	N8	N10	N1	N3	N28	N25	N21	N26	N17	N23	N24	N11	N27	N16	N22	N15	N2	N18	N6	N20
N12	70																											
N19	183	39																										
N14	217	187	13																									
N13	239	211	308	20																								
N4	238	209	313	386	17																							
N5	220	169	178	204	197	111																						
N7	220	195	232	260	267	203	53																					
N9	227	196	244	277	265	193	295	32																				
N8	219	183	234	264	264	190	282	376	19																			
N10	227	203	248	278	280	198	296	375	371	17																		
N1	195	169	226	248	245	176	256	336	329	354	20																	
N3	221	190	240	274	266	197	296	376	371	392	351	18																
N28	202	136	160	197	192	195	195	202	189	214	189	206	103															
N25	198	146	190	223	220	203	205	211	204	209	191	200	153	2														
N21	208	146	197	226	221	207	207	209	204	213	187	205	165	291	5													
N26	208	154	196	230	218	208	210	212	204	220	194	213	167	291	312	28												
N17	200	147	185	223	214	206	209	209	200	215	188	204	164	285	305	306	1											
N23	210	148	192	225	213	201	211	215	200	215	195	209	168	287	311	307	307	3										
N24	198	148	188	220	213	197	204	208	199	212	186	201	169	271	288	287	286	290	13									
N11	247	209	216	226	220	228	214	237	233	241	219	242	231	234	236	239	229	235	230	212								
N27	126	82	99	132	124	111	115	115	105	118	89	113	94	110	109	113	110	113	115	160	2							
N16	174	120	145	165	176	162	166	176	157	174	153	167	152	149	157	157	151	155	153	217	70	2						
N22	188	145	164	196	199	168	186	192	178	198	172	192	150	157	164	175	165	165	164	233	90	201	2					
N15	271	248	290	304	302	253	296	319	302	316	292	312	256	278	278	281	276	277	275	306	221	321	340	141				
N2	314	291	321	333	338	315	340	343	331	346	317	340	314	326	327	331	322	331	329	330	265	323	335	387	481			
N18	203	139	154	186	187	183	169	176	171	186	167	181	136	151	157	169	152	156	154	228	90	146	153	269	307	25		
N6	282	238	251	277	272	293	269	276	267	267	261	268	258	259	266	270	267	266	259	297	192	237	259	328	372	252	263	
N20	204	144	195	226	217	204	208	216	206	216	196	208	165	293	301	307	299	303	284	233	112	152	169	286	332	163	267	2

Comparison with Distributed Approach

- Compared attackers from NorNet setup to those in Distributed setup
  - Among 4343 NorNet attackers 1987 were found in distributed setup
- Majority of the attackers were reported by all or multiple sensors

- Analyzed attackers against different attack stages
  - Same behavior in both setups



Conclusions

- Security sensor system implemented
- Two deployment scenarios
  - Distributed approach
  - NorNet Central Sensor approach
- NorNet Testbed
  - Easy to install new sensors without additional software
- Distributed attacks were analyzed
  - Scanning of whole range of IPs or subnets
  - Same attackers observed at different sites (China, Germany and Norway)
  - Information sharing among attackers
- Outlook
  - Rules Optimization
  - Mitigation