PA197 Secure Network Design
2. Faults, Threats, Attacks

Eva Hladká, Luděk Matyska

Faculty of Informatics

March 1, 2016

Content

Faults and Failures

- All systems susceptible to failures
- Failure resilience mandatory part of the design
  - unfortunately not true for most commercial systems/networks today
  - resilience goes with a cost
  - not possible to build absolute resilience
- Faults: some flaws in the system
  - but sometimes left by design, e.g. just one router for a small network
- Failures: emergent faults
  - Random faults: occurrence unpredictable (probability)
  - Induced (domino): e.g. link disconnection leads to higher service failure
  - Malicious: results of attacks (usually use some (known) flaw)

Internet

- Physical
  - components faults and failures
  - hardware level, but includes immediate software components
    - e.g. active element operating system fault or failure
- Protocols
  - software layer
  - shortcomings (limits) of protocols
  - bugs: incidental and malicious failures
- Applications
  - software layer

Selected failure examples

- Topology failures
- Overload
- Integrity
- Software faults

Topology failures

- Cable failures
  - terrestrial
  - sub-marine
- Sub-marine cable threats
  - fishing and anchoring
  - natural disasters
    - earthquake 27th December 2006 damaged the cables near Taiwan, leading to disruption of Internet and telephone service in Asia Pacific region
    - Hong Kong completely cut off
  - theft
    - March 2007, 11 km section of cable connecting Thailand, Vietnam, and Hong Kong removed
    - Internet speed affected in Vietnam

Topology failures II

- Routing problems
  - link disconnection and/or node failure
- Router failures
  - (D)DoS attacks
  - software bugs
    - example: too long BGP Autonomous Systems paths
- Recovery times:
  - hundreds of milliseconds for intra-domain routing (e.g. OSPF)
  - minutes for inter-domain routing (BGP)
- Pakistan "black hole" in 2008 after banning YouTube
  - propagated through the mis-configuration to the whole world

Overload failures

- Result of limited capacity of network equipment
  - congestion (flash/short/long term)
- TCP has congestion control
  - however independent of routing
  - simply slowing down instead of re-routing
    - one of motivations for Software Defined Networks (SDN)
- Flash Crowds versus (D)DoS attacks
  - how to distinguish unusually high but legitimate traffic from malicious traffic?

Software faults

- Bugs in software
  - development phase
  - buffer overflow most prominent example
- Bugs in configuration
  - deployment phase
  - could have wide (global) effect
    - Pakistan/YouTube, Google search, ...

Ad-hoc, mobile and vehicular networks

- In some aspects similar to Internet
  - the mobility introduces additional complexity/source of failures
- Hardware level
  - component faults
    - more fragile “active” elements
    - frequent failure a property
  - disconnection due to distance
    - not possible to distinguish from a failure
- Protocols
  - reliable routing problem
  - link failure a property, not an exceptional event

Sensor networks

- Static nodes, but high probability of failure of any individual node
- Limited life span of a node
  - battery drainage
- Interference
- Routing and transmission protocols
  - redundancy versus energy conservation

Threats—Overview

- Physical installation threats
  - hardware threats
    - physical damage to the hardware and/or wires
  - electrical threats
    - electricity fluctuations (brownouts and spikes)
    - electricity loss (blackouts)
  - environments threats
    - external conditions (temperature, electrostatic and magnetic interferences, humidity etc)
    - disasters (flood, fire, . . .)
  - maintenance threats
    - missing, incorrect or damaged spare parts
    - incorrect or missing labeling of components and cables
    - poor handling of components
    - low quality of instalation

Internet threats

- Phishing
  - search ("fish") for personal details
  - usually using e-mails or social networks
- Viruses and worms
  - malicious software that arrives attached to another (benign) program or data (e.g. e-mail)
  - replicates within the attacked computer
  - worm actively tries to attack new systems over the network
- Spyware and adware
  - spyware collects information about users on Internet
  - adware a special kind of spyware to help targeting advertisements (without user consent)
- Trojans
  - malicious program like virus, but does not replicate itself
- Rogue security software
  - attacks trust relationship

Internet Security Threat Report

- Symantec reports
  - `https://know.elq.symantec.com/LP=1542`
- Main categories
  - mobile devices and Internet of things
  - web threats
  - social media and Scams
  - targeted attacks
  - data breaches and privacy
  - e-crime and malware
- Statistics from 2015 report

46 2014 | **57** 2013

New Android Mobile Malware Families

277 2014 | **231** 2013

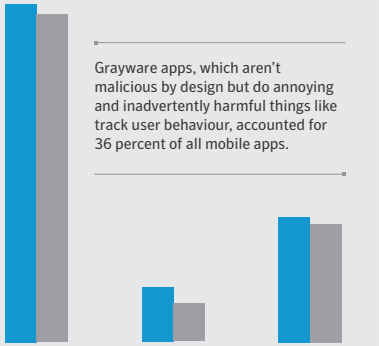
Cumulative Android Mobile Malware Families

48 2014 | **57** 2013

New Android Variants per Family

9,839 2014 | **7,612** 2013

Cumulative Android Mobile Malware Variants



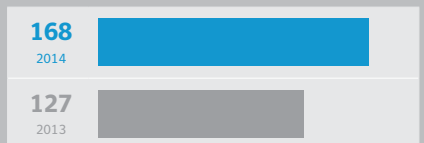
Grayware apps, which aren't malicious by design but do annoying and inadvertently harmful things like track user behaviour, accounted for 36 percent of all mobile apps.

6.3 M 2014 | **6.1 M** 2013 — Total Apps Analyzed

1 M 2014 | **.7 M** 2013 — Total Apps Classified as Malware

2.3 M 2014 | **2.2 M** 2013 — Total Apps Classified as Grayware

App Analysis by Symantec's Norton Mobile Insight



168 2014

127 2013

New Mobile Vulnerabilities

SHARE THIS

Symantec found that 17 percent of all Android apps (nearly one million total) were actually malware in disguise.

MOBILE DEVICES

Scanned Websites with Vulnerabilities

Percentage of Which Were Critical

New Vulnerabilities

Web Attacks Blocked per Day

Websites Found with Malware

Inverse Graph: Smaller Number = Greater Risk

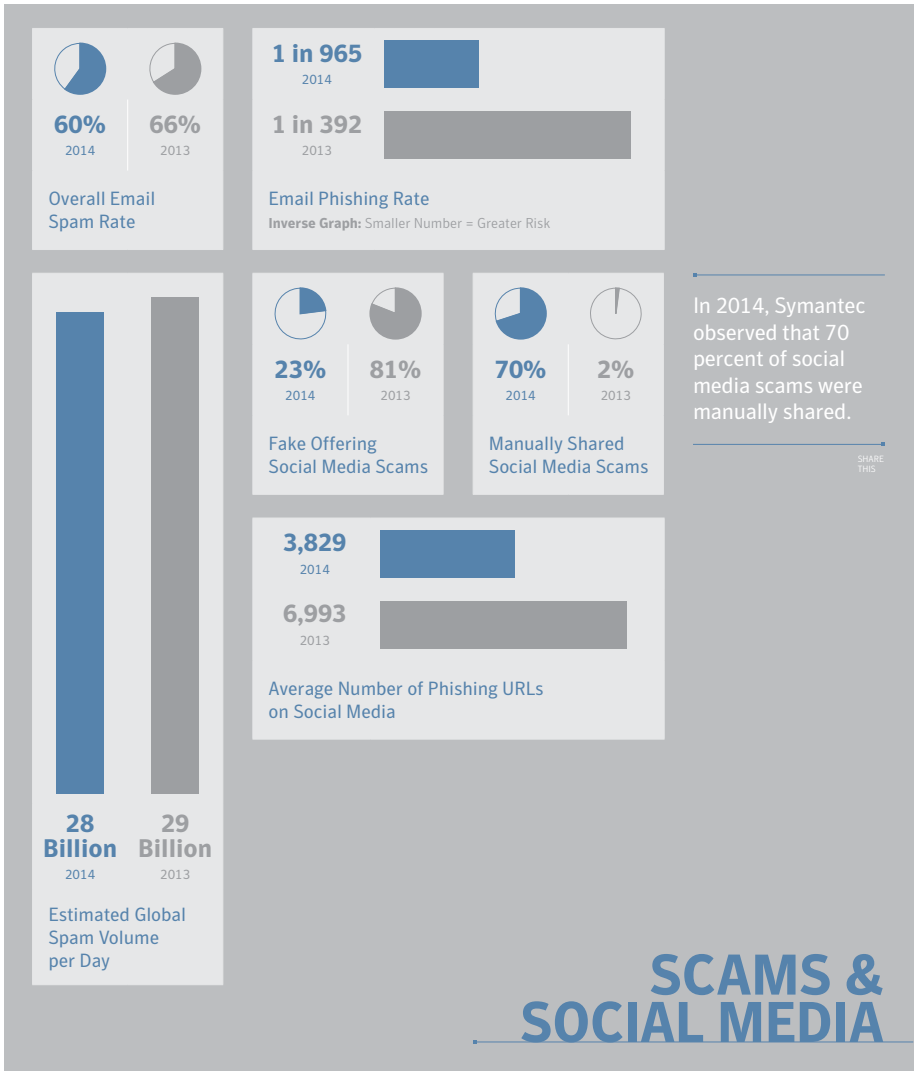
1	SSL/TLS Poodle Vulnerability
2	Cross-Site Scripting
3	SSL v2 support detected
4	SSL Weak Cipher Suites Supported
5	Invalid SSL certificate chain

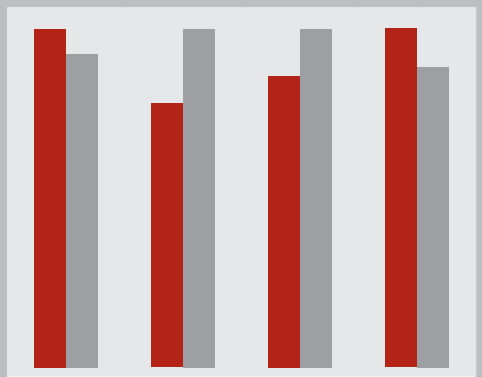
Top 5 Vulnerabilities Found Unpatched on Scanned Web Servers

Within four hours of the Heartbleed vulnerability becoming public, Symantec saw a surge of attackers stepping up to exploit it.

SHARE THIS

WEB THREATS


60%
2014
66%
2013
Overall Email Spam Rate
1 in 965
2014
1 in 392
2013
Email Phishing Rate
Inverse Graph: Smaller Number = Greater Risk
28 Billion
2014
29 Billion
2013
Estimated Global Spam Volume per Day
23%
2014
81%
2013
Fake Offering Social Media Scams
70%
2014
2%
2013
Manually Shared Social Media Scams
3,829
2014
6,993
2013
Average Number of Phishing URLs on Social Media
In 2014, Symantec observed that 70 percent of social media scams were manually shared.
SHARE THIS
SCAMS & SOCIAL MEDIA



841	779	18	23	25	29	9 Days	8 Days
Campaigns		Recipients per Campaign		Average Number of Attacks per Campaign		Average Duration of a Campaign	

Spear Phishing Email Campaigns — 2014 2013

73	83
2014	2013

Spear Phishing Emails per Day

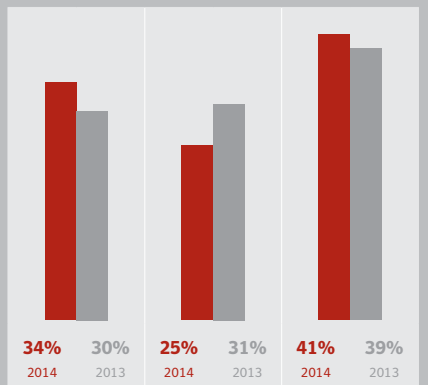
Industry	Risk Ratio	2014	2013
Mining	1 in 2.3	44%	37%
Wholesale	1 in 2.9	34%	29%
Manufacturing	1 in 3.0	33%	31%
Transportation, Communications, Electric, Gas & Sanitary Services	1 in 3.4	29%	26%
Public Administration (Government)	1 in 3.4	29%	32%

Risk Ratio of Spear-Phishing Attacks by Industry

Industry	2014	2013
Manufacturing	20%	13%
Services—Nontraditional	20%	14%
Finance, Insurance & Real Estate	18%	13%
Services—Professional	11%	15%
Wholesale	10%	5%

Top 10 Industries Targeted in Spear-Phishing Attacks

TARGETED ATTACKS



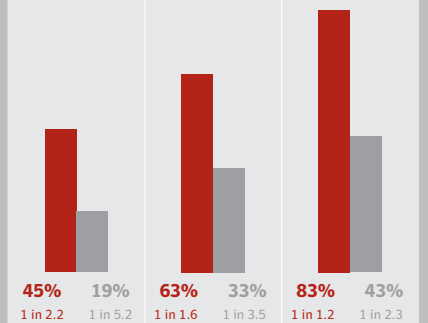
Distribution of Spear-Phishing Attacks by Organization Size

Small Businesses (SMBs) 1 to 250 Employees

Medium-Size Businesses 251 to 2,500 Employees

Large Enterprises 2,500+ Employees

Risk Ratio of Spear-Phishing Attacks by Organization Size



Individual Contributor	1 in 3.7	27%
Manager	1 in 3.8	26%
Intern	1 in 3.9	26%
Director	1 in 5.4	19%
Support	1 in 7.6	13%

Top 5 Risk Ratio of Spear-Phishing Attacks by Job Level

Sales/Marketing	1 in 2.9	35%
Finance	1 in 3.3	30%
Operations	1 in 3.8	27%
R&D	1 in 4.4	23%
IT	1 in 5.4	19%

Top 5 Risk Ratio of Spear-Phishing Attacks by Job Role

.doc	39%
.exe	23%
.scr	9%
.au3	8%
.jpg	5%

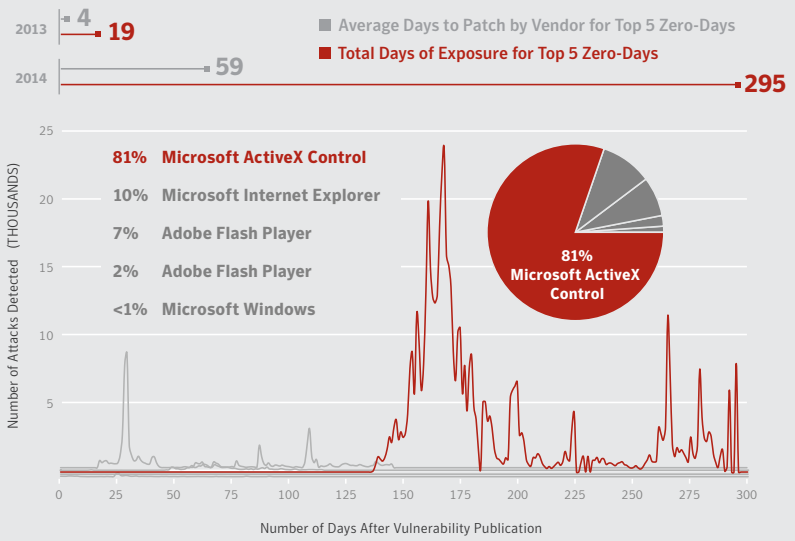
Spear-Phishing Emails Used in Targeted Attacks

Last year, 60 percent of all targeted attacks struck small- and medium-sized organizations.

SHARE THIS

In total, the top five zero-days of 2014 were actively exploited by attackers for a combined 295 days before patches were available.

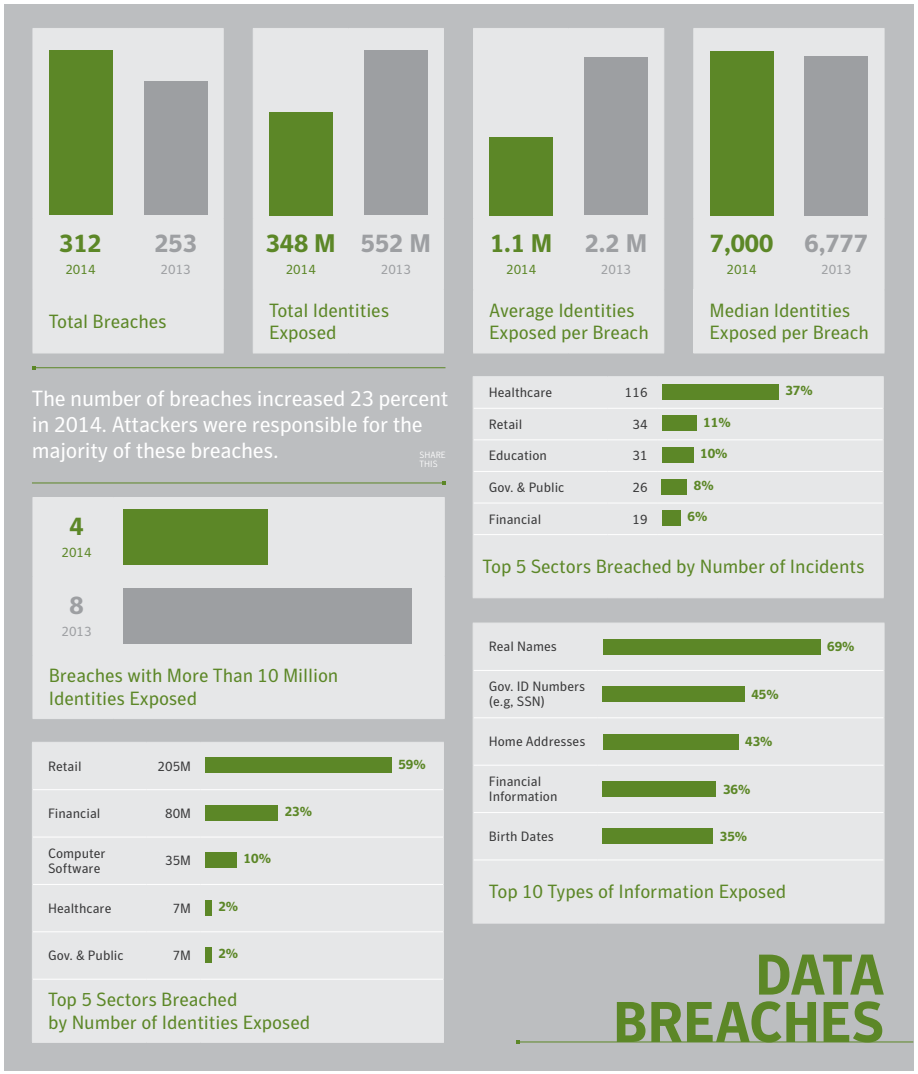
SHARE THIS



Top 5 Zero-Day Vulnerabilities – Days of Exposure and Days to Patch

Source: Symantec

Zero-Day Vulnerabilities


312
2014
253
2013
Total Breaches
348 M
2014
552 M
2013
Total Identities Exposed
1.1 M
2014
2.2 M
2013
Average Identities Exposed per Breach
7,000
2014
6,777
2013
Median Identities Exposed per Breach
The number of breaches increased 23 percent in 2014. Attackers were responsible for the majority of these breaches.
SHARE THIS
Healthcare 116 37%
Retail 34 11%
Education 31 10%
Gov. & Public 26 8%
Financial 19 6%
Top 5 Sectors Breached by Number of Incidents
4
2014
8
2013
Breaches with More Than 10 Million Identities Exposed
Real Names 69%
Gov. ID Numbers (e.g, SSN) 45%
Home Addresses 43%
Financial Information 36%
Birth Dates 35%
Top 10 Types of Information Exposed
Retail 205M 59%
Financial 80M 23%
Computer Software 35M 10%
Healthcare 7M 2%
Gov. & Public 7M 2%
Top 5 Sectors Breached by Number of Identities Exposed
DATA BREACHES

317M 2014
252M 2013
New Malware Variants (Added Each Year)

1 in 244 2014
1 in 196 2013
Email Malware Rate
Inverse Graph: Smaller Number = Greater Risk

24 K Per Day — 8.8 Million 2014
11 K Per Day — 4.1 Million 2013
Ransomware Total

Ransomware attacks grew 113 percent in 2014, along with 45 times more crypto-ransomware attacks.

Item	2014 Cost
1,000 Stolen Email Addresses	$0.50 to $10
Credit Card Details	$0.50 to $20
Scans of Real Passports	$1 to $2
Stolen Gaming Accounts	$10 to $15
Custom Malware	$12 to $3500
1,000 Social Network Followers	$2 to $12
Stolen Cloud Accounts	$7 to $8
1 Million Verified Email Spam Mail-outs	$70 to $150
Registered and Activated Russian Mobile Phone SIM Card	$100

Value of Information Sold on Black Market

1.9M 2014
2.3M 2013
Number of Bots

In 2014, up to 28 percent of all malware was “virtual machine aware.”

SHARE THIS

12% 2014
25% 2013
Email Malware as URL vs. Attachment

E-CRIME & MALWARE

Sensor networks

- Major threats:
  - physical
  - software
- Physical threats:
  - interference
  - battery drainage
  - overtake of a node
- Security
  - routing mis-information
  - data loss
  - data injection

Ad-hoc, mobile and vehicular networks

- Ad hoc network
  - a network build for a specific purpose
  - no central base stations or access points
  - each node sender/receiver
  - peer to peer and multi=hop architecture
- Mobile ad hoc network (MANET)
  - adds mobility to individual nodes
- Vehicular ad hoc network (VANET)
  - specific version of MANET
  - (semi)organized (i.e. not completely random) movement of nodes
  - Roadside Units (RSU)
    - immobile units
    - two side communication with cars
    - specific user interaction modes (drivers disturbance)

MANET Properties

- Each node can communicate
  - power constraints for nodes
- Communication is possible only between node “in range”
  - the set of neighbours changes in time
  - bandwidth usually limited
- Each node can retransmit a message
  - router capability
  - multi-hop delivery
- General performance a function of cooperation between nodes

Security problems

- Open media
  - easy to eavesdrop or interfere with
- Open routing protocol
  - no security mechanism
- Continuously changing topology
  - easy hiding for an attacker
- Relies on cooperation between devices
  - malicious node can “divert” others
- Hijacked nodes

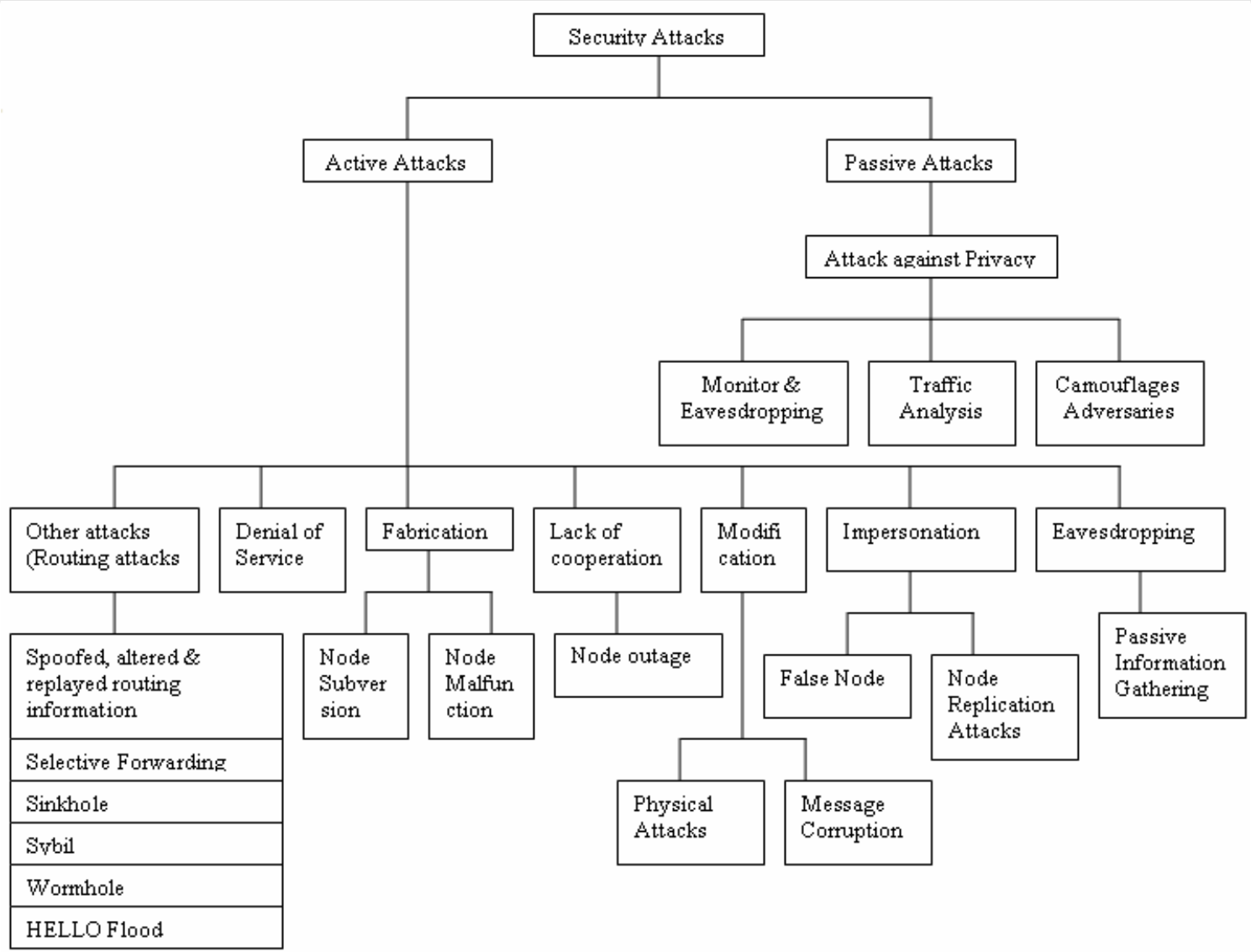
VANET specific problems

- Privacy
  - drivers identity
  - unit identification (where are they moving)
- Clear benefit for a malicious user
  - divert traffic
  - clear its own path

Basic attack modes

- Passive attacks
  - not directly influencing the target systems
  - monitoring the (unencrypted) traffic
    - authentication information (passwords)
    - other sensitive information
  - result is access to information
- Active attacks
  - break into a target system
  - bypass a security perimeter or break through it
  - manipulate messages
    - reply, modify, create, delete
  - impersonation (identity theft), Man-in-the-middle attack
  - result is access to data, modification of data, DoS

Attack typology



Sybil Attack

- Attacker assumes several identities
  - defeat trust of a reputation system
- Used to hide the malicious node (e.g. car in VANET)

Internet

- Physical attacks
  - targets the physical infrastructure
  - immediately indistinguishable form hardware faults
- Internet service attacks
  - Domain Name Service (DNS)
  - e-mail
  - protocol vulnerabilities (e.g. TCP SYN attack)
- Man-in-the-middle attack
- DoS and DDoS attacks

Other types of attack

- Insider attack
  - majority of attacks initiated from within the security perimeter
- Close-in attack
  - social engineering
  - physical access/proximity to the network
- Phishing attack
- Hijack attack
  - takes over the network session
- Exploit attacks
  - uses known security hole
- Protocol attacks
  - spoof attack
  - buffer overflow
- Password attack
  - cracking passwords: brute force and dictionary attack
  - uses access to the file/database with passwords

TCP SYN Flood Attack

- Exploits "trust" in the the TCP 3-way handshake protocol
  1. client initiates connection with SYN packet
  2. server acknowledges (SYN/ACK) and allocates resources
  3. client sends the final acknowledgment (ACK)
- What if client does not respond with ACK?
  - victim allocates resources (memory)
  - resources eventually freed through time out
  - but in the meantime victim not able to serve legitimate requests

  Simple Denial of Service attack
- Attacker does not use its own IP address
  - why?

Low Rate TCP DoS

- A paper of Kuzmanovic&Knightly: *Low-Rate TCP-Targeted Denial of Service Attacks*. SIG COMM 2003.
- Exploits TCP congestion control mechanism
- Retransmission time-out
- Exponentially reduce available bandwidth

Low Rate TCP DoS II

- Pinciples
  - mis-uses the congestion avoidance mechanism of TCP
  - if severe congestion risk is recognized, TCP reduces congestion window to one packet and waits for a period of Retransmission Time Out (RTO) after which the packets is resent
  - further loss doubles RTO period
  - short outages (on adversary flow) at around RTT force TCP to timeout; all flows *simultaneously* enter the same state
  - when TCP attempts to exit timeout and enter slow-start
  - adversary creates another outage to force the flows synchronously back to timeout state
- Difficult to detect
  - recognizable: high-rate bursts on short time-scales
- And mitigate
  - randomized minRTO

Distributed DoS

- Single source DoS attack (rather) easily defended
  - does not mean we know who is the attacker
  - but we can stop her (usually)
- Distributed DoS
  - many sources of attack
  - each harmless by its own
  - their quantity is the problem
- Uses a (huge) set of attacking machines
  - under control of attacker: bots, zombies, ...
  - innocent (secondary victims)

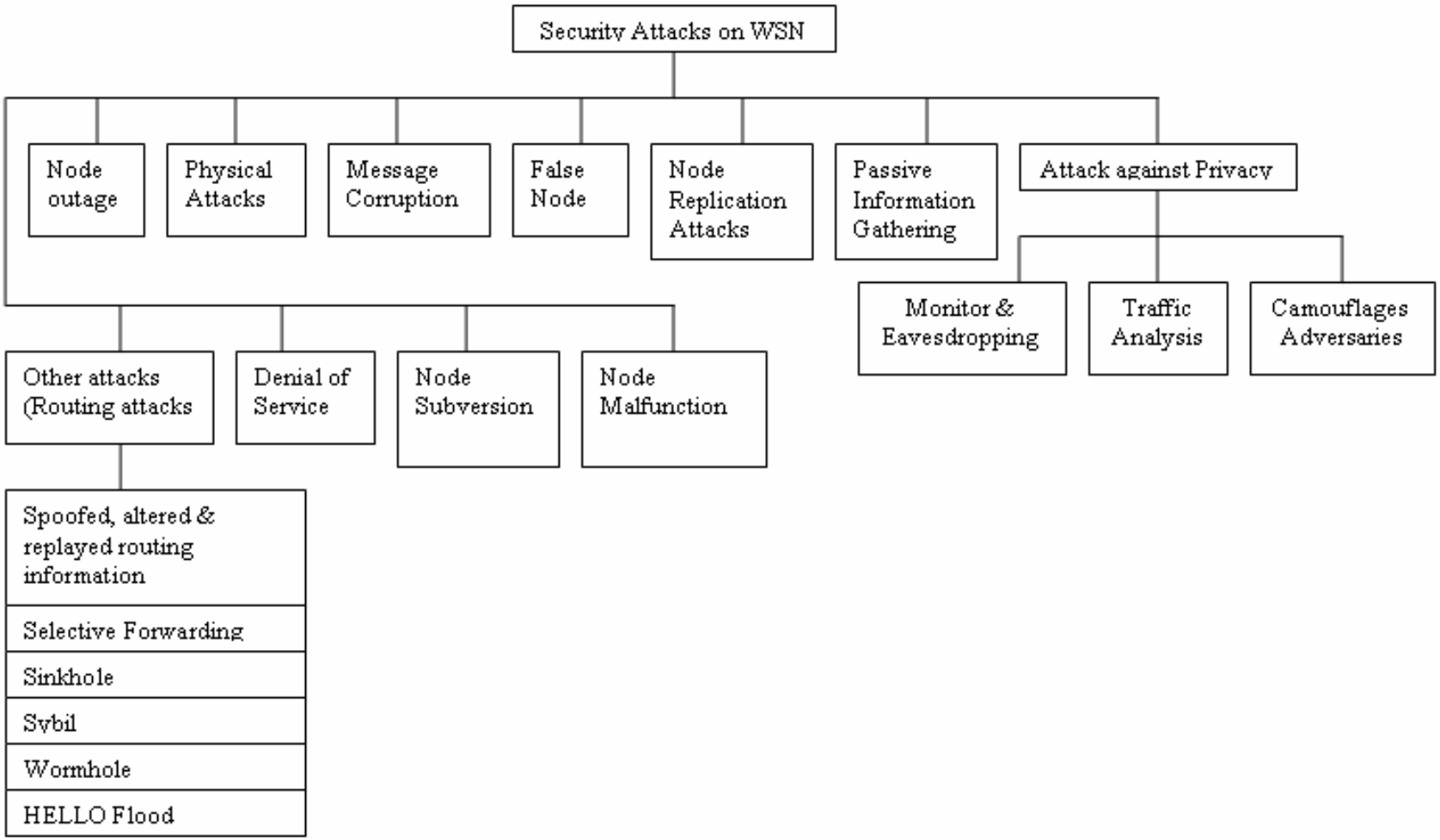
Multiple Source DDoS Attack

- Attacker controls an army of slave machines
  - result of previous successful attacks
    - legitimate owners without knowledge
  - available "on demand"
- Synchronized overload of the victim
  - sending legitimate requests from many sources
  - victim unable to differentiate the requests
    - crash of many media servers on September 11th 2001 not by attack but too extensive interest
- Usually hierarchical to hide the attacker
  - attacker directly controls only first layer of machines, these used to control the second layer, not sending the data directly to the victim

DDoS Reflector Attack

- A smaller set of machines directly controlled by attackers
- Exploits "reflector" vulnerabilities of some network protocols
  - TCP SYN Flood
  - ICMP
- Attacker send requests with forged victim's address
  - requests go to "secondary victims"—innocent machines not under attacker's control
- All responses from these secondary victims go to the primary victim$\longrightarrow$overload

Sensor networks–attack typology



Sleep Deprivation

- Also called resource consumption attack
- Overload the victim node by requests
  - route discovery
  - packets forwarding
- Exhausts internal resources
  - battery drainage
- and puts the node off-line

Ad-hoc, mobile and vehicular networks

- Passive and active attack as in other network categories
- External attacks
  - nodes that do not belong to the network
- Internal attacks
  - hijacked nodes
- Basic attack scenarios:
  - black hole, wormhole, Byzantine, sleep deprivation

Basic attacks

- Black hole attack
  - node reports route availability to targets
    - announces the shortest node
    - attracts traffic to the target node through itself
  - inspects all the packets
  - modifies, drops, delays them
- Wormhole attack
  - two cooperating malicious nodes
  - a packet collected by one are sent directly to the other ("wormhole")
  - disrupts routing when also routing control messages are tunneled
    - could prevent a discovery of any other routes

Location disclosure

- Collects information about the topology and/or structure of the network
  - route maps
- Useful for future attacks
  - important in more regular ad hoc networks like the vehicular one
  - identities of communicating parties
- Dangerous in security sensitive scenarios
  - military MANETs

Specific VANET attacks

- Sybil attacks
- Bogus information
- Denial of Service
- Impersonation (masquerading)
- Alteration attack
- Reply attack
- Illusion attack

Illusion attack

- Adversary deceives sensors in his own car to produce wrong sensor readings
  - car broadcasts false traffic warning messages
- Creates an illusion for other cars about the traffic event
- Drivers behaviour is modified
  - ultimate goal of the adversary
- Difficult to mitigate with traditional methods like trust schemes, message authentication, message integrity checks

Summary

- Provided basic classification for
  - failures and faults
  - threats
  - attacks

  for different kinds of network
  - Internet
  - sensor networks
  - ad hoc, mobile and vehicular networks
- Similarities and differences between specific networks discussed
  - random failures versus targeted use of faults
  - capacity limits
- Threats come from nature as well as from attackers
  - one issue is to properly distinguish these
  - to properly mitigate their impact
- Next lecture: Security architecture

Figure sources

- Figs.1&2 on slides 29 and 38 are taken from
  - Pamavathi et al: *A Survey of Attacks, Security Mechanisms and Challenges in WSN*. IJCIS, vol.4(1,2), 2009
    `http://arxiv.org/pdf/0909.0576.pdf`