PA197 Secure Network Design
2. Faults, Threats, Attacks

Eva Hladká, Luděk Matyska

Faculty of Informatics

February 26, 2019

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

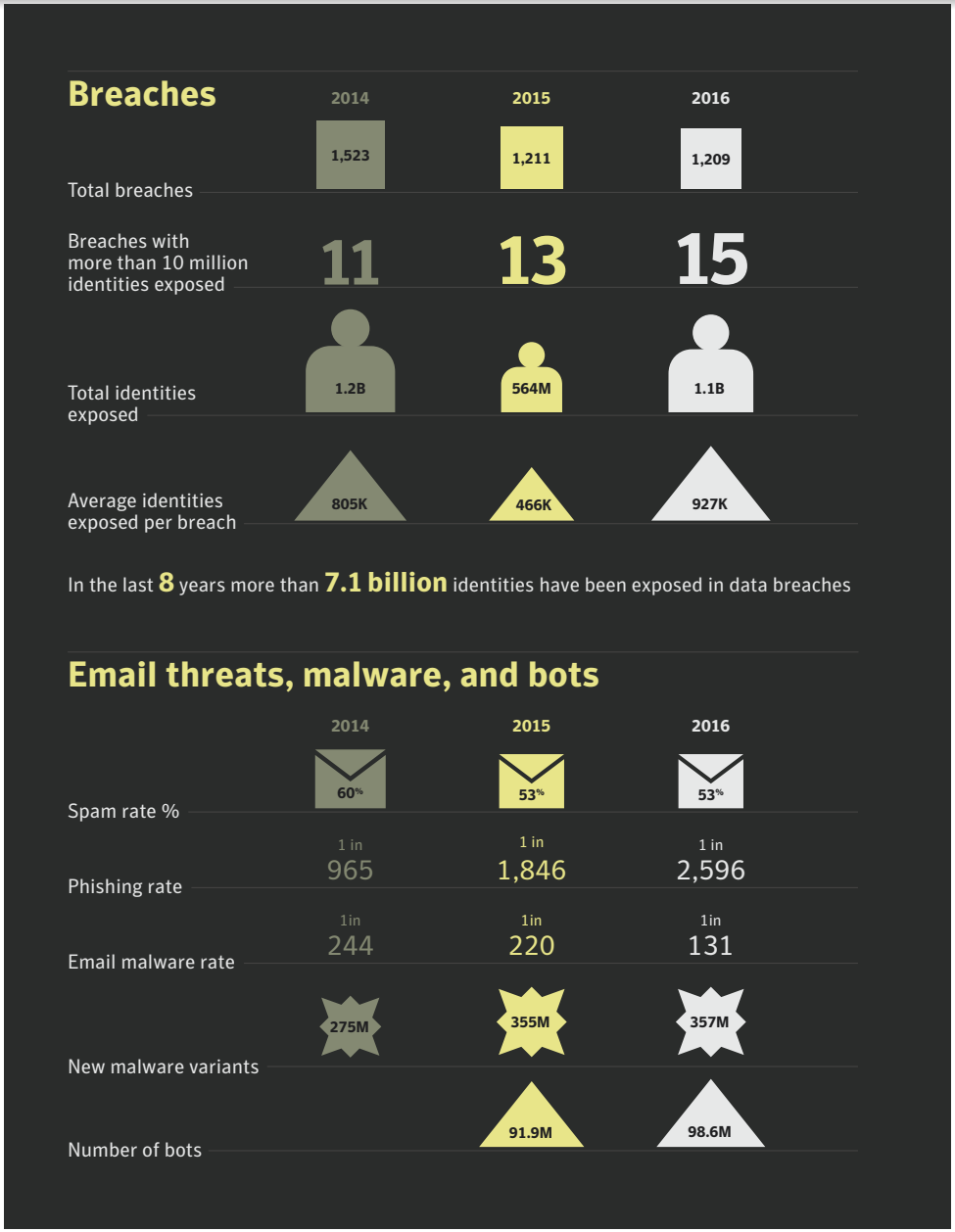
- Physical installation threats
  - hardware threats
    - physical damage to the hardware and/or wires
  - electrical threats
    - electricity fluctuations (brownouts and spikes)
    - electricity loss (blackouts)
  - environments threats
    - external conditions (temperature, electrostatic and magnetic 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

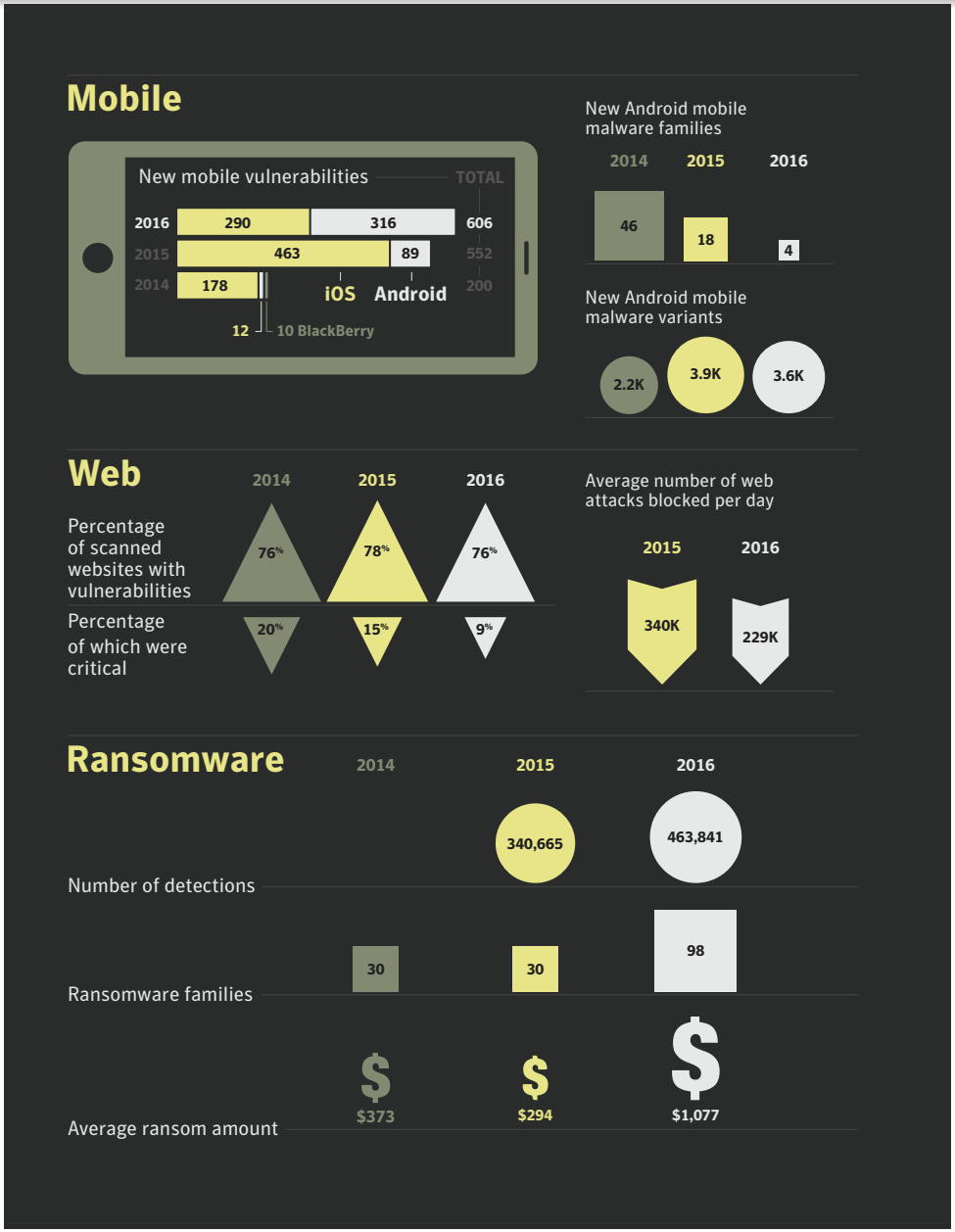
Internet threats

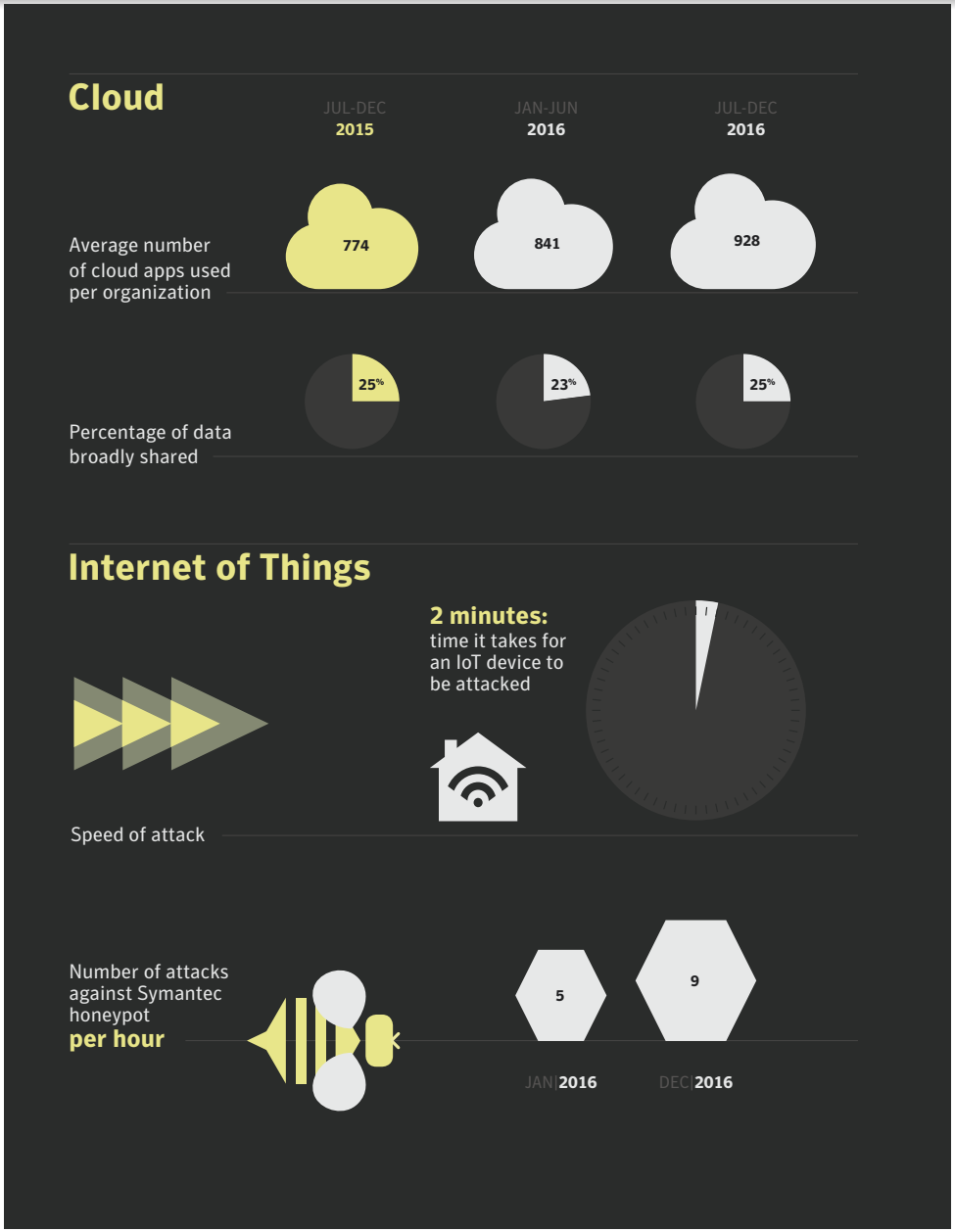
- Phishing
  - search ("fish") for personal details
  - usually using e-mails or social networks
- Viruses and worms
  - malicious software that arrives attached to another (benign) program or data (e.g. e-mail)
  - replicates within the attacked computer
  - worm actively tries to attack new systems 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
  - 2017: `https://www.websecurity.symantec.com/security-topics/istr-2017-infographic`
  - 2015: `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 2017 report


Breaches
2014
2015
2016
Total breaches
1,523
1,211
1,209
Breaches with more than 10 million identities exposed
11
13
15
Total identities exposed
1.2B
564M
1.1B
Average identities exposed per breach
805K
466K
927K
In the last 8 years more than 7.1 billion identities have been exposed in data breaches
Email threats, malware, and bots
2014
2015
2016
Spam rate %
60%
53%
53%
Phishing rate
1 in 965
1 in 1,846
1 in 2,596
Email malware rate
1in 244
1in 220
1in 131
New malware variants
275M
355M
357M
Number of bots
91.9M
98.6M


Mobile
New mobile vulnerabilities
TOTAL
2016 290 316 606
2015 463 89 552
2014 178 200
iOS
Android
12
10 BlackBerry
New Android mobile malware families
2014 2015 2016
46
18
4
New Android mobile malware variants
2.2K
3.9K
3.6K
Web
2014 2015 2016
Percentage of scanned websites with vulnerabilities
76% 78% 76%
Percentage of which were critical
20% 15% 9%
Average number of web attacks blocked per day
2015 2016
340K
229K
Ransomware
2014 2015 2016
Number of detections
340,665
463,841
Ransomware families
30
30
98
Average ransom amount
$373
$294
$1,077


Cloud
JUL-DEC 2015
JAN-JUN 2016
JUL-DEC 2016
Average number of cloud apps used per organization
774
841
928
25%
23%
25%
Percentage of data broadly shared
Internet of Things
2 minutes: time it takes for an IoT device to be attacked
Speed of attack
Number of attacks against Symantec honeypot per hour
5
9
JAN 2016
DEC 2016

Notable targeted attack groups

Sandworm

est. 2014

Possible region of origin: Russia

Aliases / *Quedagh, BE2 APT*

Tools, tactics, & procedures (TTP)
Spear phishing, vulnerabilities, zero-days, custom back door programs, destructive payloads

Motives
Espionage, sabotage

Target categories & regions
Governments, international organizations, energy, Europe, US

Recent activities
Linked to destructive attacks against Ukrainian media and energy targets

Housefly

est. 2001

Possible region of origin: US

Aliases / *Equation*

Tools, tactics, & procedures (TTP)
Watering holes, infected CD-ROMs, infected USB keys, vulnerabilities, zero-days, custom back door and information-stealing programs, worm programs

Motives
Espionage

Target categories & regions
Targets of interest to nation-state attackers

Recent activities
Breached in 2016, with tools and exploits leaked

Fritillary

est. 2010

Possible region of origin: Russia

Aliases / *Cozy Bear, Office Monkeys, EuroAPT, Cozyduke, APT29*

Tools, tactics, & procedures (TTP)
Spear phishing, custom back door programs

Motives
Espionage, subversion

Target categories & regions
Governments, think tanks, media, Europe, US

Recent activities
Associated with Democratic National Committee (DNC) attacks

Strider

est. 2011

Possible region of origin: Western

Aliases / *Remsec*

Tools, tactics, & procedures (TTP)
Advanced surveillance tool

Motives
Espionage

Target categories & regions
Embassies, airlines, Russia, China, Sweden, Belgium

Recent activities
Uncovered by Symantec in 2016

Swallowtail

est. 2007

Possible region of origin: Russia

Aliases / *Fancy Bear, APT28, Tsar Team, Sednit*

Tools, tactics, & procedures (TTP)
Spear phishing, watering holes, infected storage devices, vulnerabilities, zero-days, custom back door and information-stealing programs

Motives
Espionage, subversion

Target categories & regions
Governments, Europe, US

Recent activities
Associated with WADA and DNC hacks

Suckfly

est. 2014

Possible region of origin: China

Aliases / *None*

Tools, tactics, & procedures (TTP)
Custom back door programs signed using stolen certificates

Motives
Espionage

Target categories & regions
E-commerce, governments, technology, healthcare, financial, shipping

Recent activities
Targeted attacks using multiple stolen code-signing certificates

Cadelle

est. 2012

Possible region of origin: Iran

Aliases / *None*

Tools, tactics, & procedures (TTP)
Custom back door programs

Motives
Espionage

Target categories & regions
Airlines, telecommunications, Iranian citizens, governments, NGOs

Recent activities
Surveillance on domestic targets in Iran and orgs in the Middle East

Buckeye

est. 2009

Possible region of origin: China

Aliases / *APT3, UPS, Gothic Panda, TG-0110*

Tools, tactics, & procedures (TTP)
Spear phishing, zero-days, custom back door programs

Motives
Espionage

Target categories & regions
Military, defense industry, media, education, US, UK, Hong Kong

Recent activities
Shifted focus from Western targets to Hong Kong

Appleworm

est. 2012

Possible region of origin: North Korea

Aliases / *Lazarus*

Tools, tactics, & procedures (TTP)
Spear phishing, DDoS attacks, disk wiping, zero-days, custom back door and information-stealing programs, destructive payloads

Motives
Espionage, sabotage, subversion

Target categories & regions
Financial, military, governments, entertainment, electronics

Recent activities
Subject to disruption operations in early 2016. Links with Bangladesh Bank attackers

Tick

est. 2006

Possible region of origin: China

Aliases / *None*

Tools, tactics, & procedures (TTP)
Spear phishing, watering holes, custom back door programs

Motives
Espionage

Target categories & regions
Technology, broadcasting, aquatic engineering, Japan

Recent activities
Long-standing campaigns against targets in Japan

Symantec

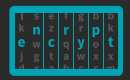
Back to Table of Contents


The underground marketplace
Ransomware toolkit
$10 – $1,800
DDoS short duration (< 1 hr)
$5 – $20
Documents (Passports, utility bills)
$1 – $3
Android banking Trojan
$200
BANK
8475 0594 5688 4856
Credit cards
$0.5 – $30
Cloud service account
$6 – $10
GIFT
Gift card
20%– 40% (of face value)
Cash-out service
10%– 20% (of acct. value)
Where everything has a price

Major ransomware threats

Locky

Cerber



CryptXXX

Approx. Ransom:

Locky	Cerber	CryptXXX
$965	$1,200	$500

Discovery:

Locky	Cerber	CryptXXX
February 2016	March 2016	April 2016

Spread through:

Locky	Cerber	CryptXXX
Email campaigns Neutrino exploit kit Nuclear exploit kit RIG exploit kit	Email campaigns RIG exploit kit Magnitude exploit kit	Angler exploit kit Neutrino exploit kit
One of the most widely spread ransomware threats in 2016 Spread via massive email campaigns powered by Necurs botnet Significant drop in Locky prevalence in early 2017 due to reduction in Necurs activity since late December 2016	Very widespread in late 2016 as a result of extensive email and RIG exploit kit campaigns Email campaigns primarily use JavaScript and Office macro downloaders but may also be attached as a zip file	Disappearance of Angler in early June 2016 prompted a drop in activity Reemerged in early 2017 delivered via Neutrino exploit kit Early variants used weak encryption which could be broken. Newer versions employ stronger encryption, making decryption impossible

Symantec

Back to Table of Contents

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 nodes "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

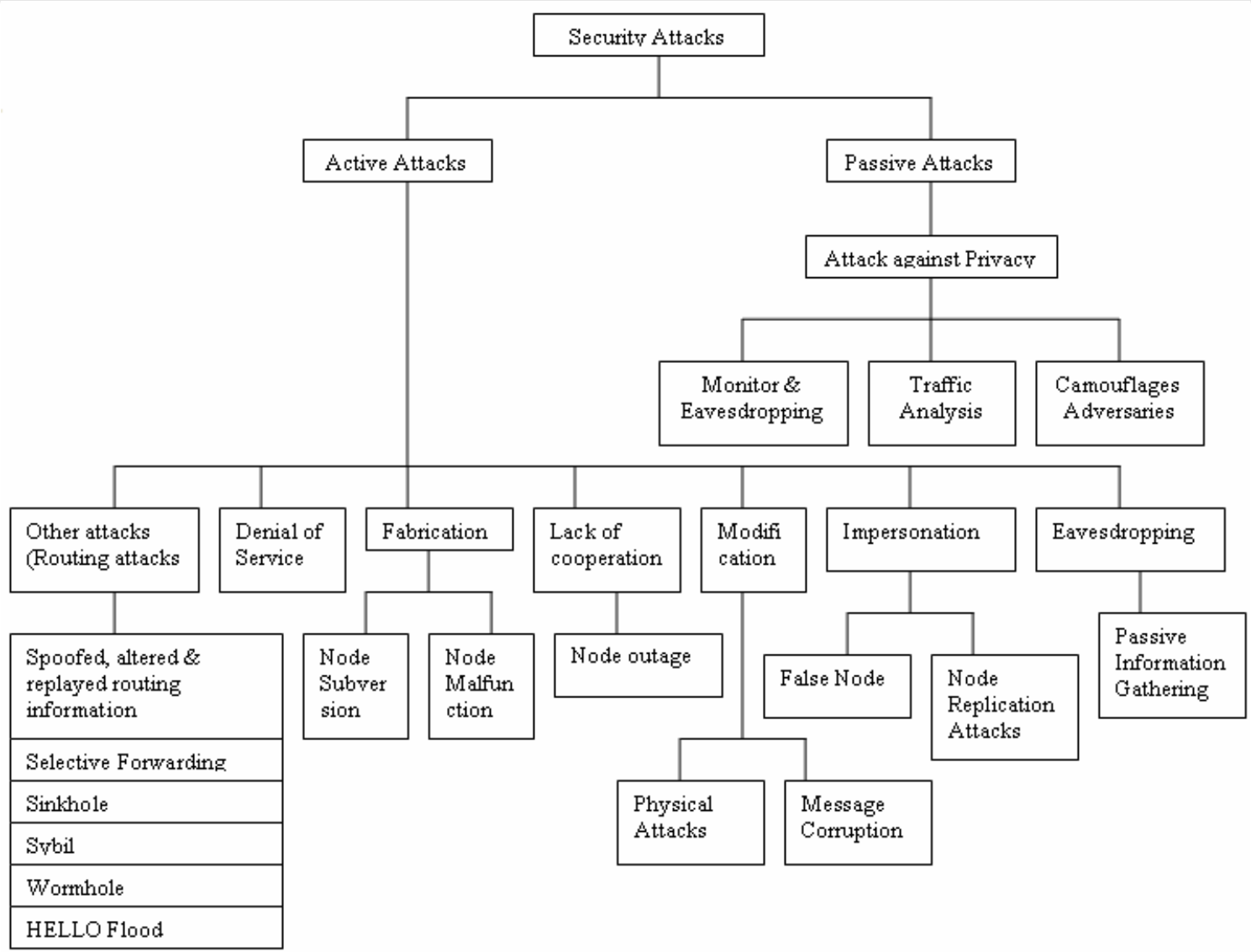
VANET specific problems

- 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)

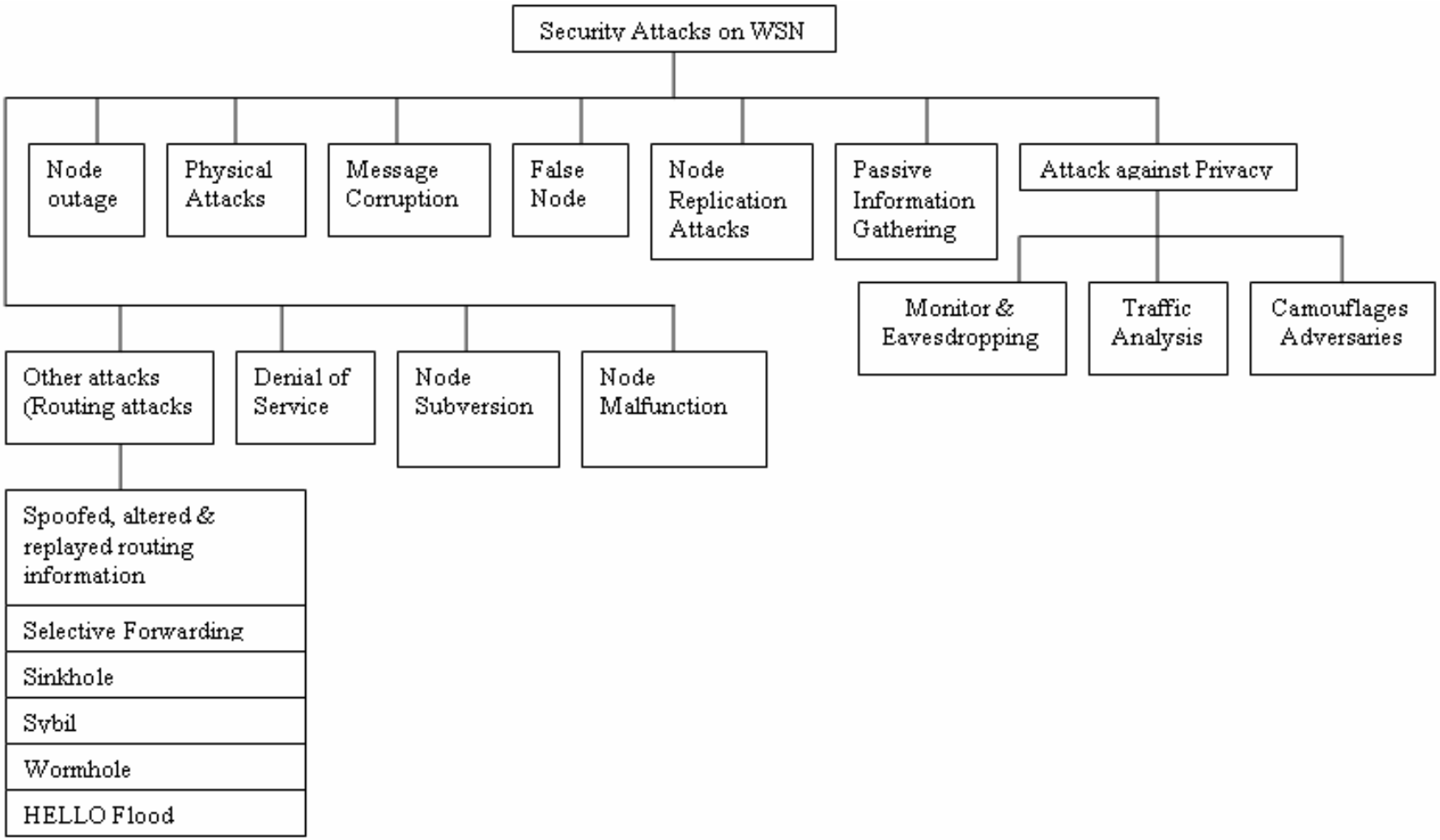
Multiple Source DDoS Attack

- 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 route
    - 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`