Network Security (NetSec)

TECHNISCHE UNIVERSITÄT DARMSTADT

Summer 2015
Chapter 01: Fundamentals
Module 05: Security Model for Networks

Prof. Dr.-Ing. Matthias Hollick

Technische Universität Darmstadt
Secure Mobile Networking Lab - SEEMOO
Department of Computer Science
Center for Advanced Security Research Darmstadt - CASED

Mornewegstr. 32
D-64293 Darmstadt, Germany
Tel.+49 6151 16-70922, Fax. +49 6151 16-70921
http://seemoo.de or http://www.seemoo.tu-darmstadt.de

Prof. Dr.-Ing. Matthias Hollick
matthias.hollick@seemoo.tu-darmstadt.de

CASED

Learning Objectives

Learning objectives

- Increase the awareness on potential attacks
  - What can go wrong?
  - How are computer networks vulnerable?
- Identify existing attacks with the network as attack vectors
  - What are some of the more prevalent attacks today?
  - Why are attacks in cyberspace fundamentally different from physical attacks?
- Derive a model for network security and network access control
- Get a first glance on protocols to secure networks

The Top Cyber Security Risks … depend on who reports these

SECURE MOBILE NETWORKING

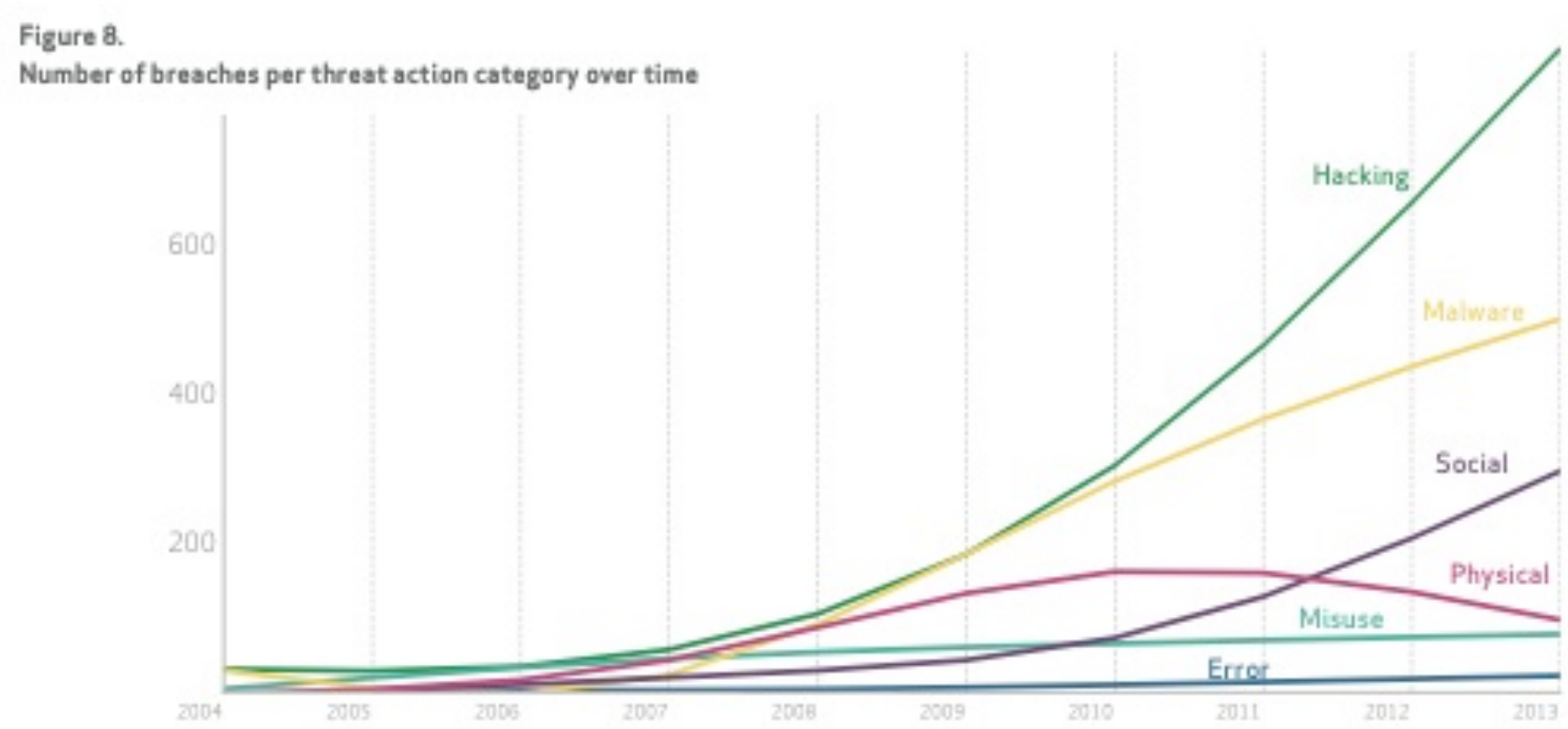
Two risks dwarf all others, but organizations fail to mitigate them

Source: http://www.sans.org/top-cyber-security-risks/
(no longer available online!)

- Priority One: Client-side software that remains unpatched
  - See also next slide
- Priority Two: Internet-facing web sites that are vulnerable

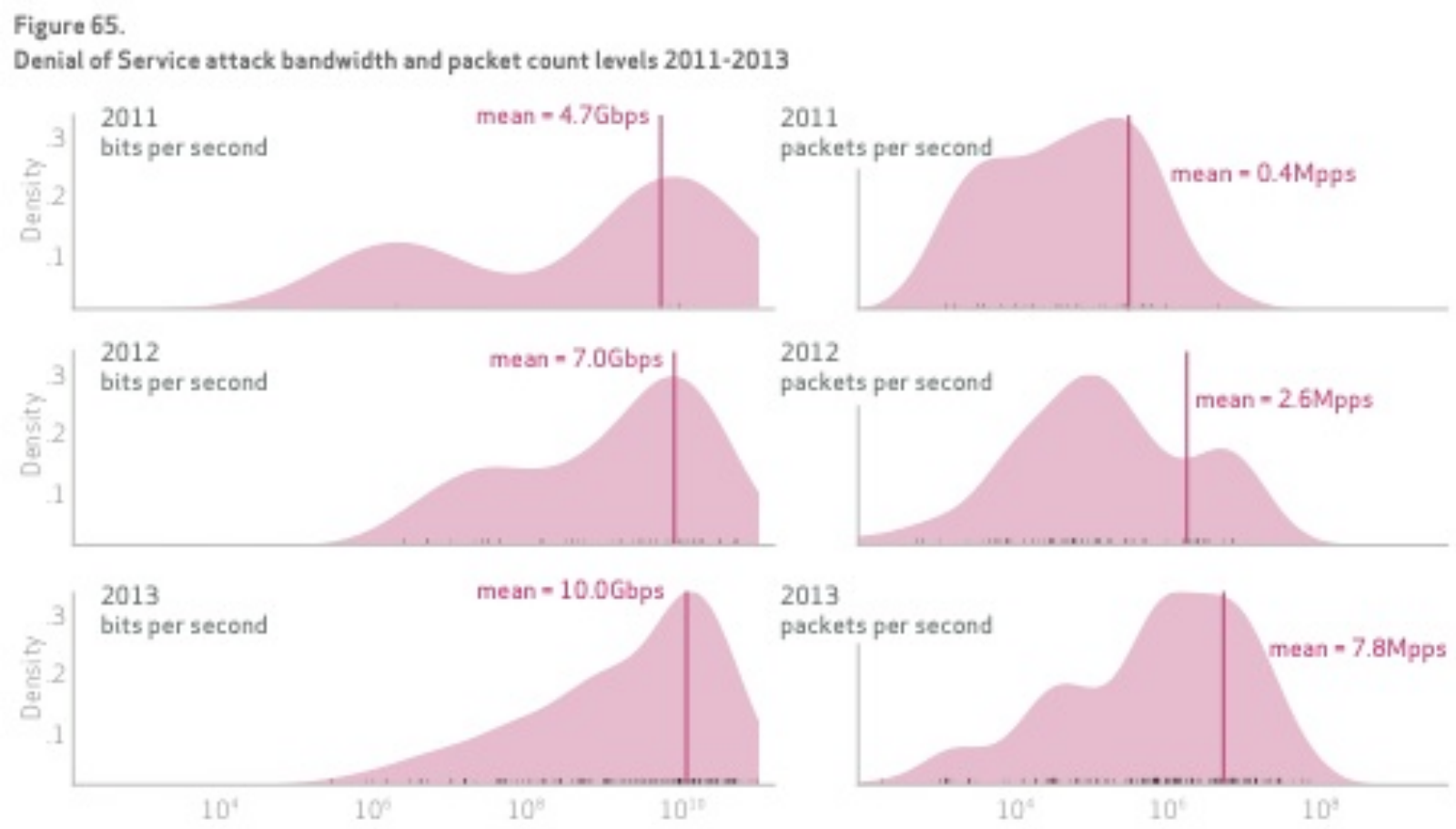
The Top Cyber Security Risks 2014 report by Verizon (also next slides)

Source: http://www.verizonenterprise.com/DBIR/2014/



The Top Cyber Security Risks 2014 report by Verizon (also next slides)

Source: http://www.verizonenterprise.com/DBIR/2014/



The Top Cyber Security Risks 2014 report by Verizon (also next slides)

Source: http://www.verizonenterprise.com/DBIR/2014/

Figure 16.
Frequency of incident classification patterns

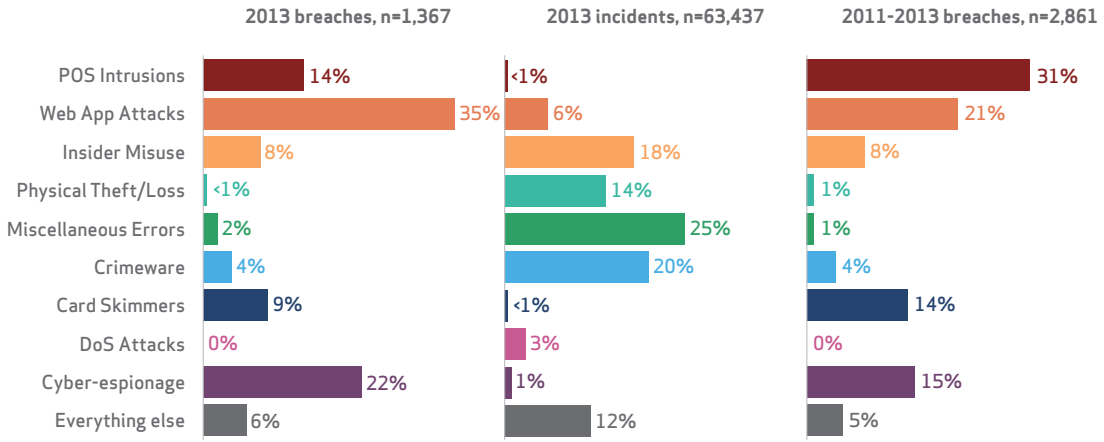


Figure 3.
Number of security incidents with confirmed data loss by victim industry and organization size, 2013 dataset

Industry	Total	Small	Large	Unknown
Accommodation [72]	137	113	21	3
Administrative [56]	7	3	3	1
Construction [23]	2	1	0	1
Education [61]	15	1	9	5
Entertainment [71]	4	3	1	0
Finance [52]	465	24	36	405
Healthcare [62]	7	4	0	3
Information [51]	31	7	6	18
Management [55]	1	1	0	0
Manufacturing [31,32,33]	59	6	12	41
Mining [21]	10	0	7	3
Professional [54]	75	13	5	57
Public [92]	175	16	26	133
Real Estate [53]	4	2	0	2
Retail [44,45]	148	35	11	102
Trade [42]	3	2	0	1
Transportation [48,49]	10	2	4	4
Utilities [22]	80	2	0	78
Other [81]	8	6	0	2
Unknown	126	2	3	121
Total	**1,367**	**243**	**144**	**980**

Small = organizations with less than 1,000 employees,
Large = organization with 1,000+ employees

Figure 9.
Top 20 varieties of threat actions over time

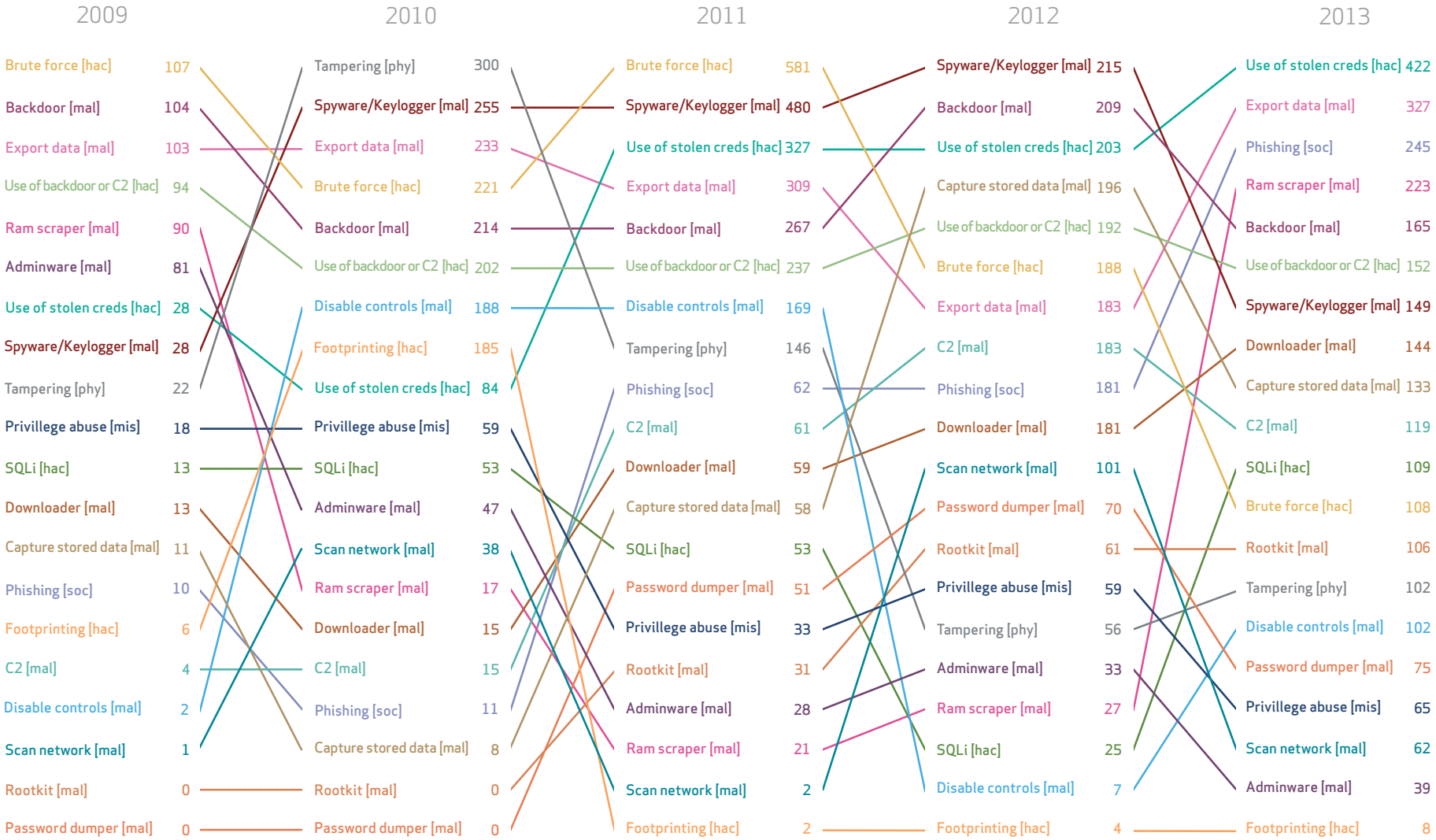
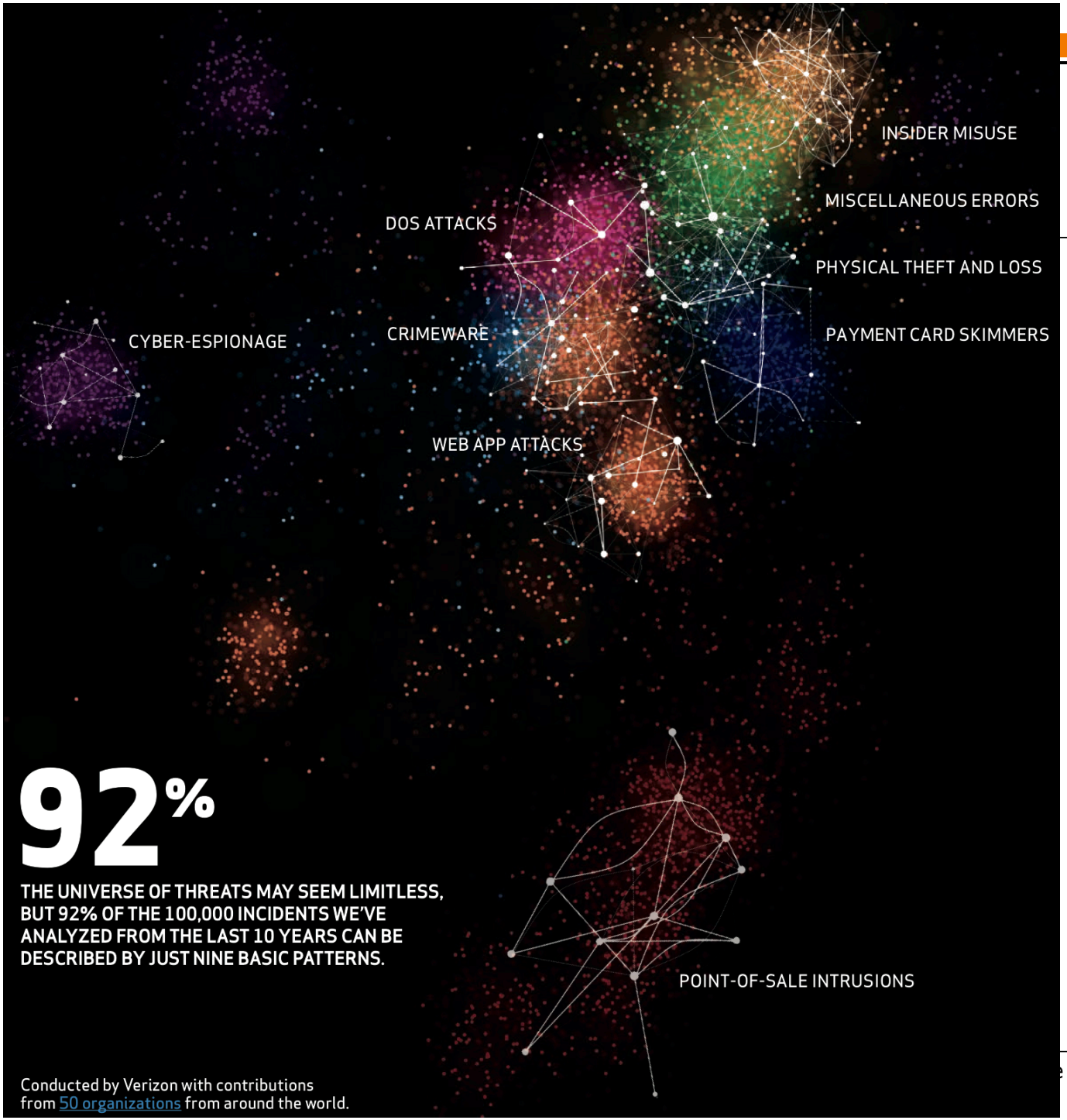


Figure 9 dives deeper into the specific varieties of threat actions observed over the last five years. The overall top twenty across the five-year span is listed in successive columns, and the lines connecting columns highlight how each action changes over time.. To be honest, concise commentary on this visualization may be impossible. Yes, it's incredibly busy, but it's also incredibly information-dense. Let your eyes adjust and then explore whatever strikes your fancy. As an example, follow RAM scrapers through the years. They start at #5 in 2009, drop way down over the next few years and then shoot up the charts to the #4 spot in 2013. We talk about that resurgence in the POS intrusions section of this report. Literally every item in Figure 9 has a story if you care to look for it. Enjoy.



SEEMO
SECURE MOBILE NETWORKING

CASED
TECHNISCHE UNIVERSITÄT DARMSTADT

Overview of this Module

(1) Networks under attack
(2) A model for network security
(3) A model for network access security
(4) Which means can be used to secure communications (on protocol level)
(5) Recommended readings

Chapter 01, Module 05

SECURE MOBILE NETWORKING

Insecure ...

Who are the Attackers?

The bad guys can put malware into your host via the Internet

We connect our hosts to the Internet to get good stuff:

- E-mail, web pages, mp3s, video clips, search results, social networking content, etc.

But along with the good stuff, comes the malware, which can:

- Delete files
- Install spyware that collects private info
- Enroll our compromised host in a botnet
  - Thousands of similarly compromised devices which can be leveraged for DDoS attacks and spam distribution

Malware: Self-replicating

Once it infects one host:

- seeks entry into other hosts
- and then into yet more hosts

Virus

- Requires some form of human interaction to spread
- Classic example: E-mail viruses

Worms

- No user interaction needed
- Worm in infected host scans IP addresses and port numbers, looking for vulnerable processes to infect

Trojan horse

- Hidden, devious part of some otherwise useful software

There are more of these digital pests

The bad guys can attack servers & network infrastructure

SECURE MOBILE NETWORKING

(Distributed) Denial of Service - (D)DoS:

- Diminishes usability of network host, network, or network infrastructure.
- Which flavors do you know?

Vulnerability attack:

- Attacker sends well-crafted messages to a vulnerable app or OS, crashing service or host.

Bandwidth flooding:

- Attacker sends a deluge of packets to the targeted host. Target's access link becomes clogged.

Connection flooding:

- The attacker establishes large number of half- or fully-open TCP connections at the target host. Target becomes incapable of accepting legitimate connections.

The bad guys can sniff packets

Passive sniffers near wireless transmitters

- We will have a special exercise on this

Wired environments too

- Many LANs broadcast
- Residential cable access systems broadcast
- Bad guys with access to internal network infrastructure can install sniffers

Packet sniffers are passive

- And therefore difficult to detect

The bad guys can masquerade as someone you trust

Easy to create packet w/ arbitrary source address, & dest address

- then transmit packet into the Internet
- which forwards the packet to its destination.

The bad guys can modify or delete messages

- Man-in-the-middle: bad guy inserted in path between two communicating entities
- Sniff, inject, modify, delete packets
- Compromise integrity of data sent btwn 2 entities

How did the Internet get to be such an insecure place?

Originally for a group of mutually trusting users attached to a transparent network.

- By definition, no need for security

Mutual trust

- By default, can send a packet to any other user
- IP source address taken by default to be true

Today, communication between trusted users is the exception rather than the rule

Secure ...

How to Make a System Trustworthy

SECURE MOBILE NETWORKING

Specification

- A statement of desired functions

Design

- A translation of specifications to a set of components

Implementation

- Realization of a system that satisfies the design

Assurance

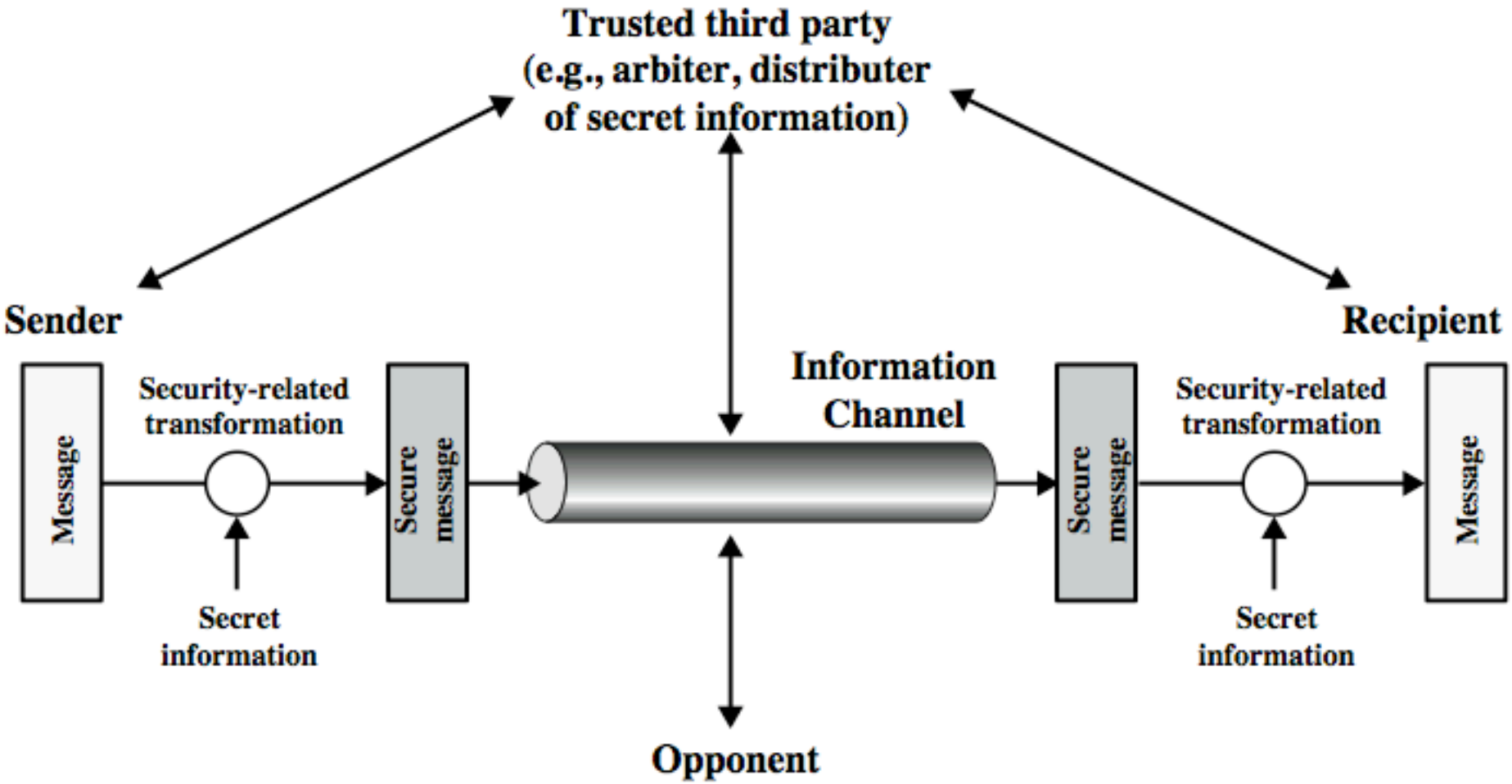
- The process to insure that the above steps are carried out correctly
- Inspections, proofs, testing, etc.

Security is a process (Bruce Schneier)

The iterations of

- Threats, Policy, Specification, Design, Implementation, Operation and maintenance

Model for Network Security



Source: book of Stallings

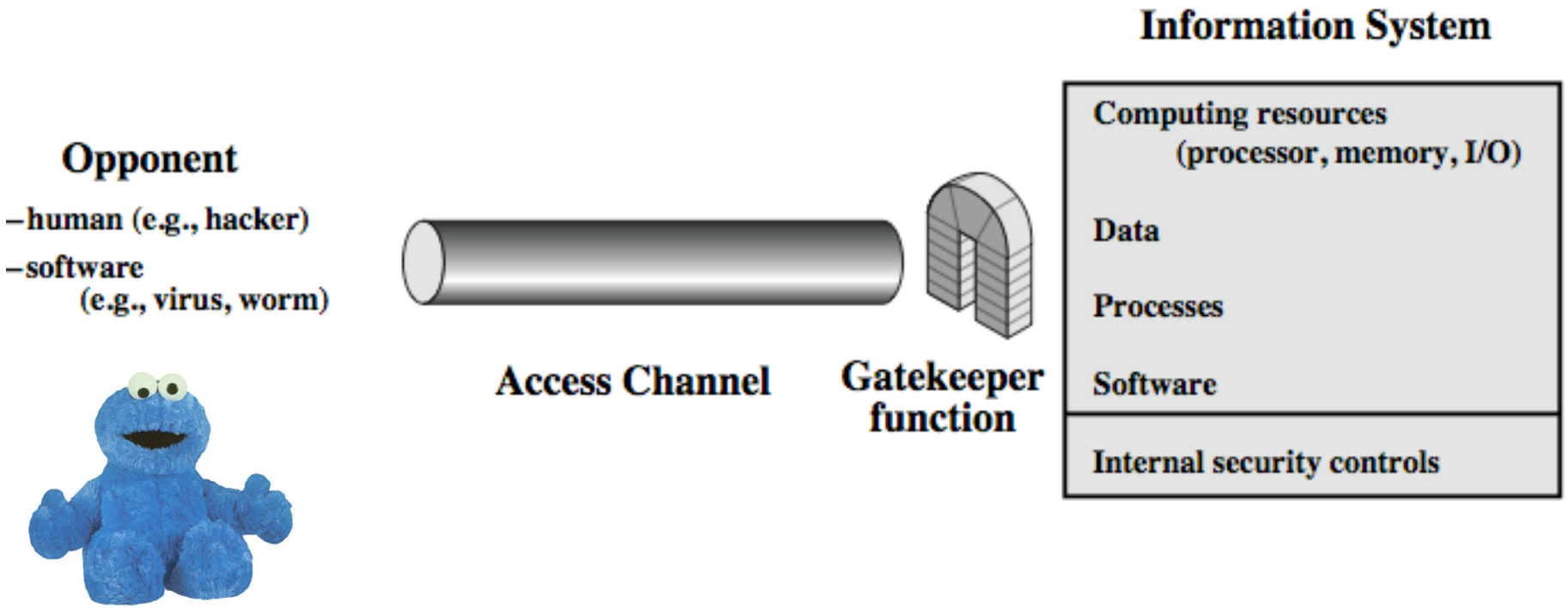
Model for Network Security

Using this model requires us to:

- Design a suitable algorithm for the security transformation
- Generate the secret information (keys) used by the algorithm
- Develop methods to distribute and share the secret information
- Specify a protocol enabling the principals to use the transformation and secret information for a security service

Input on these four basic tasks is given throughout the crypto course at TU Darmstadt

Model for Network Access Security (Controlled Access)



Source: book of Stallings

Model for Network Access Security

Using this model requires us to:

- Select appropriate gatekeeper functions to identify users
- Implement security controls to ensure only authorised users access designated information or resources

Trusted computer systems can be used to implement this model

- However, trusted platforms are rather the exception than the norm in today's networks

Network Security

SEEMOO
SECURE MOBILE NETWORKING

Which means to secure communication networks do you know?

„Different horses for different courses“ …

Source: www.sxc.hu

Which Network Security Protocols Do You Know?

SECURE MOBILE NETWORKING

	Protocols
Layer 5	
Layer 4	
Layer 3	
Layer 2	
Layer 1	

Which Network Security Protocols Do You Know?

SECURE MOBILE NETWORKING

	Protocols
Layer 5 - APP	SHTTP, S/MIME, PGP, X.400, X.500, DNS Security, Key Mgmt., etc.
Layer 4 - TRANS	SSL, TLS, SSH, TLSP
Layer 3 - NET	IPSec (AH, ESP), NLSP
Layer 2 - LINK	PPTP, L2TP, WEP, WPA, WPAv2
Layer 1 - PHY	Synchronous Link

Summary

There Is No Holy Grail of Network Security

- Never forget: Viruses, Trojan horses, ... and Users
  - Reside on higher layers (above ISO/OSI application layer)
  - Are not affected by protocol mechanisms on layers 1 to 5

Acks & Recommended Reading

Selected slides of this chapter courtesy of

- Keith Ross
- Radia Perlman
- Lawrie Brown (based on the book of William Stallings)

Recommended reading

- [KaPeSp2002] Charlie Kaufman, Radia Perlman, Mike Speciner: Network Security – Private Communication in a Public World, 2nd Edition, Prentice Hall, 2002, ISBN: 978-0-14-046019-6
- [Stallings2011] William Stallings, Network Security Essentials, 4th Edition, Prentice Hall, 2011, ISBN: 978-0-146-10805-4
- [Stallings2011b] William Stallings, Lawrence Brown, Computer Security: Principles and Practices, Pearson Education, 2011, ISBN: 978-0-273-76449-6

Copyright Notice

Contact

Prof. Dr.-Ing. Matthias Hollick
Department of Computer Science

SEEMOO
Mornewegstr. 32
64293 Darmstadt/Germany
matthias.hollick@seemoo.tu-darmstadt.de

Phone +49 6151 16-70920
Fax +49 6151 16-70921
www.seemoo.tu-darmstadt.de