Resilient Networking

Thorsten Strufe

Disclaimer: this course has been created with very valuable input from Günter Schäfer, Mathias Fischer, and the members of the Chair.

Dresden, SS 18
Lecture Outline

Who are we?
Organizational matters (preliminaries)
Course outline

A brief introduction
Who is Who

Professur „Datenschutz und Datensicherheit“
For this lecture:
• Thorsten Strufe (Lectures)
  • INF 3070 / +49 351 463 38247
  • thorsten.strufe [at] tu-dresden.de

Teaching assistants
• This lecture doesn’t have one.

Consultation:
• Send me an Email (repeatedly...)

https://tud.de/inf/ps
What We’re Interested In

- Can we prevent surveillance and retain our privacy?
- How can networks be made robust and secure?
- How can you socialize with confidentiality?
- Can we provide competitive (useful and performant) services without snooping on the users?
  - Social Networking?
  - Recommendation Systems?
- How can we analyse this context and develop sustainable solutions (scientifically)?
- With everything getting digital: how can we avoid the next big data-loss desaster?  [1] [2] [3]
The fields we’re working on

**Surveillance Prevention**
- Anonymous Communication
- Darknets
- Social network privacy

**Network Security**
- Network resilience
- SDN/NFV security
- Reactive security
- Secure Network Coding

**Data Analysis**
- Social Media Usage
- User behavior understanding
- Dynamic complex graphs
- Inference prevention

**System Security**
- Distributed Clouds
- Protocol/Service partitioning
- Trusted Execution Env. (sgx)
- Component-based software

18.04.2018
What we offer you

<table>
<thead>
<tr>
<th>FS</th>
<th>Wintersemester</th>
<th>FS</th>
<th>Sommersemester</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>2</td>
<td>Informations- und Kodierungstheorie</td>
</tr>
<tr>
<td>3</td>
<td>Betriebssysteme &amp; Sicherheit</td>
<td>4</td>
<td>Forschungslinie</td>
</tr>
<tr>
<td>5</td>
<td>BAS-4 SaC-1 / Kanalkodierung</td>
<td>6</td>
<td>BAS-4 SaC-2/Crypto</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>8</td>
<td>Vert-4, ANW/AFT, Beleg SaC-2/Crypto/Resilient Networking</td>
</tr>
<tr>
<td>9</td>
<td>Vert-4, ANW/AFT Kanalkodierung</td>
<td>10</td>
<td>Diplomarbeit</td>
</tr>
</tbody>
</table>

**BAS-4:**
- **Security & Crypto 1**
- **S&C 2 (PETs)**
- **Crypto**
- **Kanalkodierung**

**Vert-4:**
- **S&C 1&2**
- **Crypto**
- **Resilient Networking**
- **Kanalkodierung**

**B-510/B-520:**
- **S&C 1/2**
- **Kanalkodierung**
- **Seminare/Praktika**

https://tu-dresden.de/ing/informatik/sya/ps/studium

18.04.2018
Some Words Regarding this Course

Main topic of the course is the security of deployed, crucial networks, networking functions, and network protocols.

Considering the Internet: networking is an essential service, hence the networking infrastructure is/may be the main target of attacks!

Now what!? 
1. Introduction
2. Graphs and graph theory
3. Crypto basics (Symmetric/Asymmetric/MACs)
4. Link-Layer Security
5. Resilient Routing (Attacks on BGP, SBGP)
6. IPsec
7. TLS
8. DNS Security
9. DDoS and Countermeasures
10. Resilient Overlay Networks / Blockchain / Darknets
11. Intrusion Detection and Response
Organizational Matters

There will be some ex-cathedra parts, but please ask and discuss as much as possible!

Course Language
- Slides are in English, presentation as you prefer
- => What's your language of preference?

Slide history
- Based on several former courses given at TU Ilmenau, Uni Mannheim, and TU Darmstadt
- Heavily derived from „Network Security“ and „Protection of Communication Infrastructures“ of/with Prof. Schäfer in Ilmenau and extended with Prof. Fischer's input from Hamburg

18.04.2018
Slides/recordings will be on the Web site

Literature/References

- Schäfer, Roßberg: Network Security
- For crypto: Dan Boneh’s coursera course
- David Kahn: The Codebreakers
- Simon Singh: The Code Book
Organizational matters

Courses
• Mo 14:50 – 15:20
• E010

Exercises
• Wed 14:50 – 15:20
• E009 (starts now, first meeting in CW 19: May 10, prepare now)

Exams
• Oral exams, make appointments
• Procedure:
  • Questions available in German (and English upon request)
  • Answers given in German (and English upon request)
• No written material allowed (books, slides, notes)
  • Except language dictionaries for non-native speakers (German/English), *without* any personal annotations, handwritten comments, supplements, etc.
  • If needed, we will provide a list of important equations

All necessary information (will be) on the Web site
Exercise course will be organized as a reading group
  • Papers (links) available on the webpage (soon)

  • Read papers early...

  • One paper with relation to lecture topics will be presented (by a random **one of you**) and discussed (by **you**) each week (please take note of the emphasize on **YOU :-)**

Intention of the reading group is to learn
- from good (and bad) scientific papers
- how to stay up to date and inform yourselves at the source
- that what others do is mostly no rocket science
- how to read a paper properly (for sure not in the order from beginning to the end!)

Different kinds of papers

**Papers:** the classic form of scientific content spreading, a single contribution
- **Workshops:** Early ideas, WiP, Challenges/discussions ("Recurring issues with spark-plug electrodes")
- **Conferences:** concise studies ("On the electrode shapes in spark-plug design")

**Journal articles:** self-contained ("On spark-plug design")
**Surveys:** summarizing a field or research area
The Reading Group – Reviewing Papers

Paper idea
• What is the field of research?
• What is the motivation of the paper?
• What is the problem the paper tries to solve?
• What is the exact research question?
• What is (are) the paper hypotheses?
• How relevant is this research?

Paper content
• What is the claim, what are the assumptions of the paper?
• Which definitions are contained?
• What is the idea for solving the problem?
• Which implications does it entail?
• How is the evaluation carried out? Does it suffice to demonstrate/substantiate the claims? What about the results?

Critical acclaim: Merits & Shortcomings
A Survey of Covert Channels and Countermeasures in Computer Network Protocols

Sebastian Zander and Grenville Armitage, and Philip Branch, Swinburne University of Technology Melbourne, Australia

Abstract

Covert channels are used for the secret transfer of information. Encryption only protects communication from being decoded by unauthorised parties, whereas covert channels aim to hide the very existence of the communication. Initially, covert channels were identified as a security threat on monolithic systems i.e. mainframes. More recently focus has shifted towards covert channels in computer network protocols. The low entropy of data and use of unnumbered packets in the Internet...
What is the field of research? What is the exact problem domain?

Survey content
- What are the assumptions in the survey? Which definitions are used?
- Aspects, requirements, concepts, properties?
- Which classification is developed and used?
- Which implications does each class entail?

Critical acclaim
- How convincing are classification and implications?
- Completeness of the survey
- Merits & shortcomings
Questions?
Introducing Actors of the Play

For clarity it’s good to have some model...

The SaC 1 – scenario:

The RN – scenario:
A word on assumptions.
Assume an omnipotent adversary. She could:
• access all information of interest
• compromise arbitrary intermediate systems
• physically destroy any or all components

Could we deal with this?
Unfortunately, no:
„Nothing can protect from an omnipotent adversary.“

More realistic (specific!) model of adversaries needed.
An **adversary model** needs to define

- **The intention** of the adversary
  - Break and/or access *<something>*

- **The behavior**
  - Passive or active?

- **The capabilities** of an attacker
  - Computational capacity (often: think complexity class)
  - Resources (time and money)

- **The area of control**
  - Insider or outsider?
  - Local, regional, or global?
Mallory has full control over the communication channel:
- Intercept/eavesdrop on messages (passive)
- Relay messages
- Suppress message delivery
- Replay messages
- Manipulate messages
- Exchange messages
- Forge messages

But:
- Mallory *can't* break (secure) cryptographic primitives!
Let’s get started!

“Always on”, ubiquitous connectivity to the global Internet has dramatically changed the way we
– communicate,
– conduct business, and
– organize our society

CPS, connected cars, and pervasive computing promise to create an additional layer of networked devices

However, the benefits associated with information and communication technology imply new vulnerabilities

The modern information society exhibits an increasing dependence on availability and secure operation of communication services
What are „Resilient Networks“?

“Resilience is the ability of an object to spring back into shape”

“Resilience is the ability of the network to provide and maintain an adequate level of service in the face of challenges to normal operation”

“Resilience is the ability of the network to provide and maintain an acceptable level of security service in case some nodes are compromised.”

Challenges? Compromised nodes...?

What kind of problems, challenges, threats could you imagine?

What exactly do these terms mean, anyway?

Sterbenz: Resilinets, 2006-2008
Abstract Definition:

- A threat is any possible event or sequence of actions that might lead to a violation of one or more security goals.
- The actual realization of a threat is called an attack.

Examples:

- A hacker breaking into a corporate computer.
- Disclosure of emails in transit.
- A hacker temporarily shutting down a website.
- Someone using services or ordering goods in the name of others.
- ...

What are security goals?

- Security goals can be defined:
  - depending on the application environment, or
  - in a more general, technical way.
Security Goals in Application Environments

Public Telecommunication Providers:
- Protect subscribers’ privacy
- Restrict access to administrative functions to authorized personnel
- Protect against service interruptions

Corporate / Private Networks:
- Protect corporate confidentiality / individual privacy
- Ensure message authenticity
- Protect against service interruptions

All Networks:
- Prevent outside penetrations (who wants hackers?)

Security goals are also called *security objectives*
Security Goals Technically Defined (CIA)

**Confidentiality:**
- Data transmitted or stored should only be revealed to the intended audience
- **Confidentiality of entities** is also referred to as **anonymity**

(Data) **Integrity:**
- It should be possible to detect any modification of data
- This requires to be able to identify the creator of some data

**Availability:**
- Services should be available and function correctly

**Accountability:**
- It should be possible to identify the entity responsible for any communication event

**Controlled Access:**
- Only authorized entities should be able to access certain services or information

Several other models have been proposed, anything beyond CIA is constantly subject to arguments and discussions...
Threats Technically Defined

**Masquerade:**
- An entity claims to be another entity

**Eavesdropping:**
- An entity reads information it is not intended to read

**Authorization violation:**
- An entity uses a service or resources it is not intended to use

**Loss or Modification of (transmitted) information:**
- Data is being altered or destroyed

**Denial of Communication Acts (Repudiation):**
- An entity falsely denies its participation in a communication act

**Forgery of information:**
- An entity creates new information in the name of another entity

**Sabotage:**
- Any action that aims to reduce the availability and / or correct functioning of services or systems
Security Service:

• An abstract “service” seeking to ensure a specific security property

• Can be realised with the help of cryptographic algorithms and protocols or with conventional means:
  - Keep electronic document on a floppy disk confidential by storing it on the disk in an encrypted format or locking away the disk in a safe
  - Usually a combination of cryptographic and other means is most effective
A Bit More Terminology: Crypto-*

**Cryptographic Algorithm:**
- A mathematical transformation of input data (e.g. data, key) to output data
- Cryptographic algorithms are used in cryptographic protocols

**Cryptographic Protocol:**
- A series of steps and message exchanges between multiple entities in order to achieve a specific security objective

**Cipher:** a tuple of algorithms to en- and decrypt

**Plain-/Ciphertext**

**Credentials, Keys, and Keying material**
Security Services – Overview

**Authentication**
- Ensure that an entity has in fact the identity it claims to have

**Integrity**
- Ensure that data created by specific entity isn’t modified
  *without detection*

**Confidentiality**
- Ensure the secrecy of protected data

**Access Control**
- Ensure that each entity accesses only services and information it is entitled to

**Non Repudiation**
- Prevent entities participating in a communication exchange from later falsely denying that the exchange occurred
To find countermeasures, threats have to be evaluated appropriately for a given network configuration.

Therefore, a detailed network security analysis is needed that:

• evaluates the **risk potential** of the general threats to the entities using a network, and
• estimates the **expenditure** (resources, time, etc.) needed to perform known attacks.

→ Attention: *It is generally impossible to assess unknown attacks!*
Architectural View of the Threatened “Object”

Communication in Layered Protocol Architectures
Security Analysis of Layered Protocol Architectures 1

Dimension 1: At which interface could an attack take place?
Security Analysis of Layered Protocol Architectures 2

Dimension 2: In which layer could an attack take place?
Generally, attack techniques are based on:

- **Passive** behaviour:
  - Eavesdropping

- **Active** behaviour:
  - Delay of PDUs (Protocol Data Units)
  - Replay of PDUs
  - Deletion of PDUs
  - Modification of PDUs
  - Insertion of PDUs

*All have to be considered for security analyses!*
One approach: produce arbitrary threat list by any ad-hoc brainstorming method

Example: Hospital Information System
- Corruption of patient medical information
- Corruption of billing information
- Disclosure of confidential patient information
- Compromise of internal schedules
- Unavailability of confidential patient information
- ...

Drawbacks of this approach:
- Questionable completeness of identified threats
- Lack of rationale for identified threats other than experience
- Potential inconsistencies (e.g. disclosure vs. unavailability of confidential patient information in the example above)
A threat tree is a tree with:

- **nodes** describing threats at different levels of abstractions, and
- **subtrees** refining the threat of the node they are rooted at,
- where the child nodes of one node give a complete refinement of the threat represented by the parent node

Technique for establishing threat trees:

- **Start** with general, abstract description of complete set of threats for a given system (e.g. “security of system X compromised”)
- **Iteratively**, gradually introduce detail by carefully refining the description
- Each node becomes root of a **subtree** describing threats represented by it
- Eventually, each **leaf node** of the tree provides a description of a threat that can be used for a (less arbitrary) threat list

The main idea of this technique is to postpone the creation of (arbitrary) threat lists as much as possible
Example: A Hospital Information System Threat Tree

Hospital System Threats

Patient Medical Information
- Life Threatening
  - ... 
  - Disclosure
  - Integrity
  - Denial of Service
- Non Life Threatening
  - ... 

Non Patient Medical Information
- Billing
  - ... 
- Non Billing
  - ... 

At each level of refinement the child nodes of a node **must** maintain demonstrable completeness to allow for confidence that nothing is missing

(source: [Amo94])
Child nodes can have different relations to their parent nodes

The two most common relations are AND and OR:

These relations can be used to infer composed threat:

- Augment nodes with effort estimations (e.g. easy, moderate, high)
- OR-related composed threat inferred as the lowest effort value subtree (the attacker will most likely take the easy way...)
- For conjunction, infer highest effort (all threats have to be realized)
Supporting System Security Engineering with Threat Trees

Appropriate attributes are, e.g., estimated \textit{criticality} and attacker \textit{effort} for individual threats. Threat trees then can help to gain insight where to spend resources to decrease the overall system’s vulnerability:

- The second threat tree re-evaluates the risk after some protective measure has been taken to increase the attacker’s effort for subthreat B.
- Here, risk is assessed as: \[ Risk = \frac{\text{Criticality}}{\text{Effort}} \]
Summary
(High Level System Security Engineering Process)

• Specify system architecture:
  – Identify components and interrelations

• **Identify threats**, vulnerabilities and attack techniques:
  – The threat tree technique provides help for this step

• **Estimate** component **risks** by adding attributes to the threat tree:
  – However, removing subjectivity from initial assessments is often impossible and other attributes than criticality and effort (e.g. risk of detection) might have to be considered as well

• Prioritize **vulnerabilities**:
  – Taking into account the components’ importance

• Identify and install **safeguards**:
  – Apply protection techniques to counter high priority vulnerabilities

• Perform potential **iterations** of this process
  – Re-assess risks of the modified system and decide, if more iterations are required
Countering Attacks: Three Action Classes

**Prevention:**
- Measures taken to avert that an attacker succeeds in realizing a threat
- Examples:
  - Cryptography: encryption, computation of modification detection codes, running authentication protocols, etc.
  - Firewalls: packet filtering, service proxying, etc.

**Detection:**
- Measures taken to recognize an attack while or after it occurred
- Examples:
  - Recording and analysis of audit trails
  - On-the-fly traffic monitoring

**Reaction:**
- Measures taken in order react to ongoing (mitigation and healing) or past attacks
- Examples:
  - Adding new firewall rules
  - Traffic re-routing

(DDS: Prevention, Removal, Forecasting, Tolerance/Graceful degradation)
This course tackles the following aspects:

- Threats to and measures for ensuring *availability*
- Threats and measures concerning systems (beyond pure network security protocols which are more targeting transmission security)
- Measures for intrusion detection and response

*Considering the Internet: networking is an essential service, hence the networking infrastructure is/may be the main target of attacks! We’ll hence be looking at the security of deployed, crucial networks, networking functions, and network protocols.*
You know who we are

You know what to expect from the lecture

You have seen some trends that are happening

You have been introduced to Alice, Bob, Eve, and Mallory

You understand what threats are ... and what this means

You can tell security goals (CIA!) from security services

You know how to perform a network security analysis using threat trees ;-)