ETH zürich

Zurich Information Security and Privacy Center (ZISC)

Annual Review 2019

ETH Zurich, Zurich Information Security and Privacy Center (ZISC)

Introduction

Information Society of Tomorrow

The world is undergoing a dramatic transformation from the industrial society of the 20th century to the information society of the 21st. New information technologies and services emerge at a rapid pace and these innovations have a significant impact on our social, political, and economic lives. The change does not come without risks. Interruption of services can threaten lives and properties, corruption of information can disrupt the work of governments and corporations, and disclosure of secrets can damage individuals as well as institutions. These threats are no longer limited to hobbyists hackers; instead we witness attacks from organized crime, terrorists and governments. To counter such risks in the constantly evolving information technology landscape, we need a thorough understanding on the theoretical foundations of information security, as well as practical attacks and countermeasures.

Research Center

The Zurich Information Security and Privacy Center (ZISC) is an industry-supported research center of ETH Zurich, founded in 2003. The goal of ZISC is to bring academia and industry together to solve the information security challenges of tomorrow. In ZISC, PhD students and senior researchers perform academic research under the supervision of ETH Zurich faculty members. Many ZISC research projects are done in co-operation with an industry partner.

Education

Besides research, ZISC provides world-class academic education in information security. This includes training through projects, classes at ETH Zurich, and workshops for ZISC researchers and industry partners.

Why a Security Center in Zurich?

Zurich is a center of global banking and insurance, two industries that have particularly strong security needs and whose success inherently depends on their reputation as being secure. Zurich also hosts many leading technology companies that develop novel security and privacy solutions. Finally, Zurich is centrally situated in the heart of Europe. The goal of ZISC is to establish a critical mass of information security talent and research in Zurich that benefits academia, economy and society.

News and Activities 2019

During 2019, the ZISC center expanded its research activities by starting out several new research projects. The topics of these new projects range from secure governance of blockchains to robotics and route optimization. Many of the new projects are carried out in cooperation with an industry partner company which helps the ETH researchers to steer their research focus and enables ETH researchers to test their research results in realistic production environments. More about these projects will be explained in the following pages of this brochure.

As on previous years, ZISC center has also continued its strong involvement with both the local and global research community. As an example of local involvement, numerous scientific talks were organized as part of our weekly series of technical talks, called the ZISC lunch seminar.

The list of speakers included world-leading experts and researchers. These talks are open to ETH researchers and industry partners alike. As an example of international involvement, the ZISC center helped to organized the annual summer school on real-world crypto and privacy at Sibenik, Croatia and continued its support to the ETH Studio initiative at New York City in collaboration with Cornell Tech.

During 2019, Professor Kenny Paterson joined the ZISC faculty. Prof. Paterson's research expertise is in applied cryptography and he has made numerous high-profile research results related to practically-oriented topics like TLS security. Prof. Paterson's added expertise will further strengthen the research competence of ZISC center for the following years to come.

Partners

The research activities of the ZISC center are supported by these partner companies

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

armasuisse

NEC

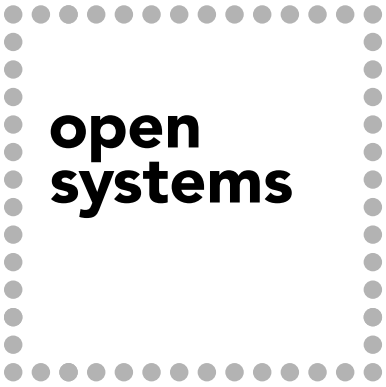
Zürcher Kantonalbank

ZURICH

SIX

SWISS POST

Associate Partner



Research Highlights 2019

LightningFilter: Traffic Filtering at 100 Gbps

During the past year, the Network Security Group has focused on developing systems to improve the availability in the Internet.
In the face of widespread distributed denial-of-service (DDoS) attacks, flooding both network links and end hosts, this is a crucial building block of a future Internet architecture like SCION.

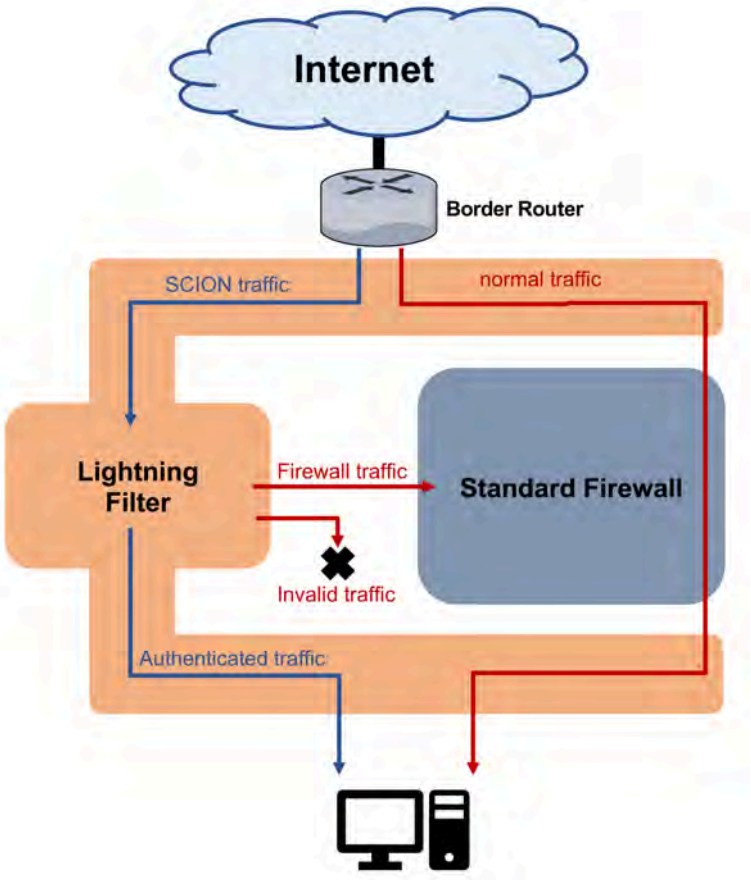
One important component of the DDoS-defense mechanisms is the defense of end hosts. In today's Internet, many users and companies rely on firewalls to protect internal networks from malicious traffic.

However, firewall hardware that is able to process large amounts of traffic (on the order of 100 Gbps) is very expensive and can cost several hundreds of thousands of Swiss francs.

Nevertheless, these systems not only suffer from false alarms but they are unable to detect many types of malicious traffic.

To overcome these issues, researchers at the Network Security Group have developed LightningFilter, a system that uses highly efficient cryptography and a novel key-derivation mechanism to authenticate the source of packets at very high speeds.

In addition to performing source authentication, LightningFilter can detect and block duplicated traffic and enforce rate limiting.



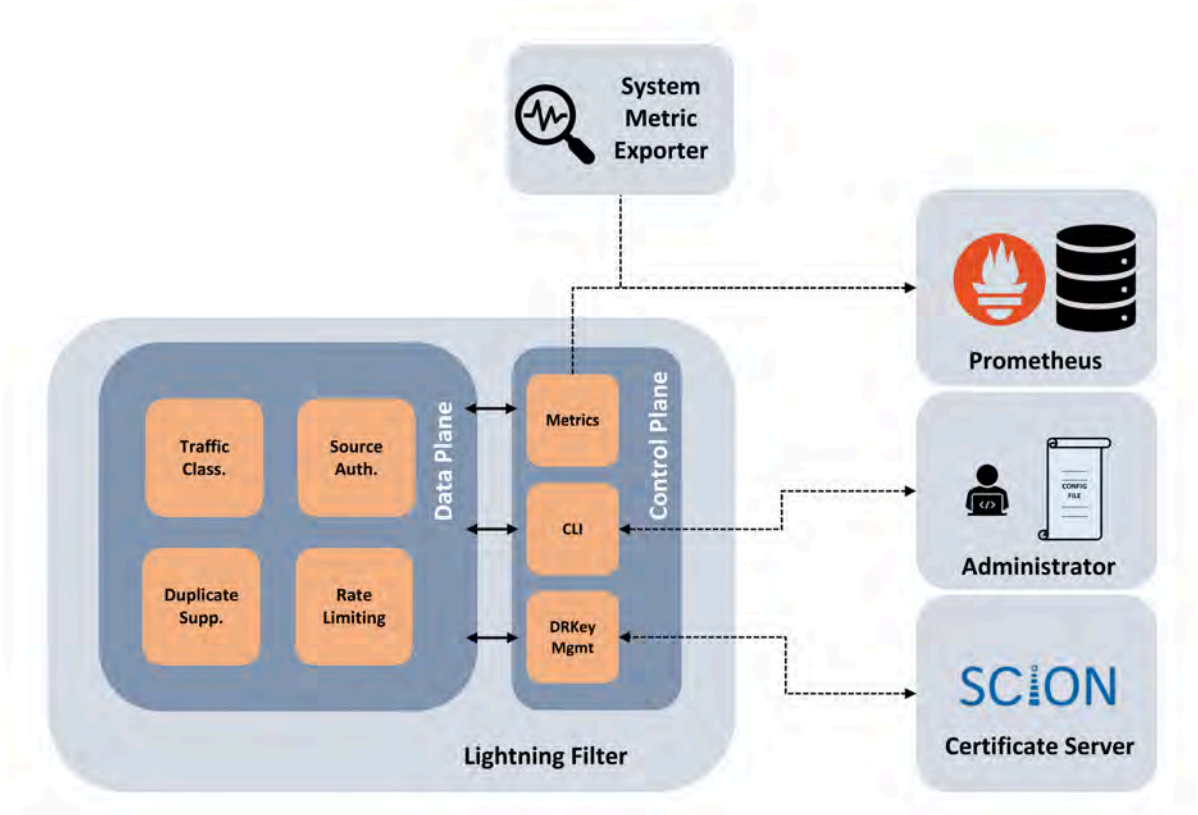
It can be managed and configured easily through a command-line interface and provides monitoring information through Prometheus/Grafana.

After processing by LightningFilter, authenticated packets from trusted sources, which are expected to represent the majority of incoming traffic, can then bypass the standard firewall and directly reach the internal network. Only the small remainder of the traffic, unauthenticed packets or packets from untrusted sources, need to be additionally processed.

This severely decreases the resource requirements for the standard firewall and can lead to drastic cost reductions.

A proof-of-concept implementation of LightningFilter produced exciting measurements.
Running on commodity hardware, the system is able to process, authenticate, and filter traffic at rates of 120 gigabit per second and defend against typical DDoS attack scenarios.

We expect LightningFilter to be a disruptive technology that, at the same time, increases security and reduces costs for hosts in a future Internet.



Research Highlights 2019

Formal Verification of the Secure Network Architecture SCION

The current Internet suffers from a deeply-rooted lack of scalability, reliability and security. Despite decades of research, no straightforward solution is in sight, and calls for **a clean-slate redesign of the Internet** are gaining traction. The SCION architecture was developed by Adrian Perrig, ETH Professor for Network Security, as a response to this challenge. SCION relies on highly efficient cryptographic packet validation for scalable, reliable and secure forwarding.

> The SCION packet forwarding protocol has been carefully designed and tested. Testing alone, however, cannot exhaustively cover all possible protocol executions and thus cannot rule out all attacks.

By contrast, **mathematical proofs of security hold for all possible protocol executions**, assuming that the verified model accurately abstracts the real system and environment. Such proofs can be constructed using formal verification techniques.

This is the domain of ETH researchers headed by David Basin, Professor for Information Security.

The team has used state-of-the-art formal verification techniques and tools to model and verify the SCION's packet forwarding, as part of a larger effort to verify the SCION architecture. This principled approach models system components, the network environment, and the adversary, and formalizes the desired properties. In the case of SCION, the attacker is a colluding Dolev-Yao attacker that controls part of the network.

The properties are path authorization and detectability: The first asserts that each packet only traverses the network along paths authorized by all on-path entities. This rules out routing loops and uneconomical paths.

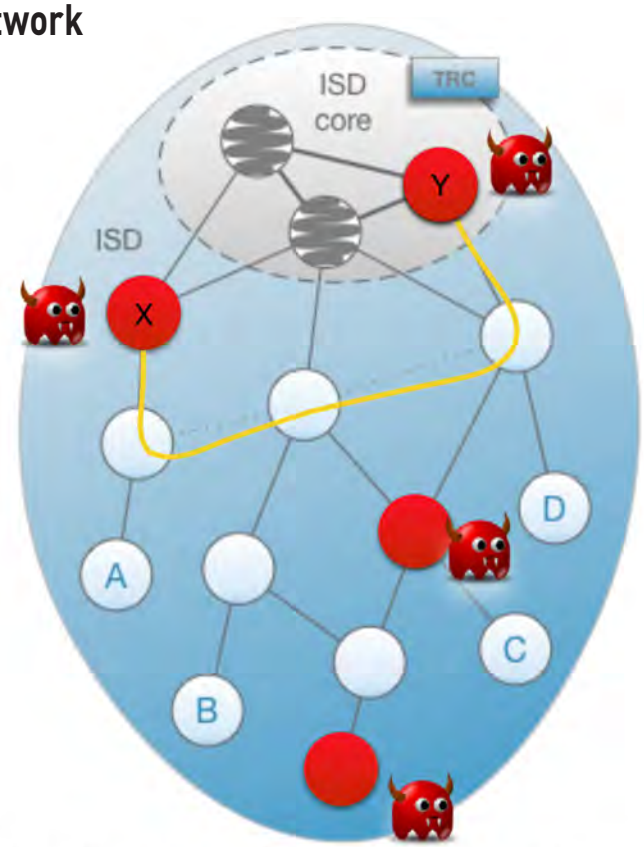
The second states that a malicious on-path entity cannot hide its presence on the path.

The properties are formalized in higher-order logic and the model is developed in an interactive theorem prover using refinement. Refinement breaks the proof down into small steps that can be verified by both humans and machines.

The two properties presented above were proven. **This process revealed several security-relevant weaknesses that were resolved quickly, and in close collaboration with SCION protocol designers and the implementation team**.

The security proofs also aided in the precise understanding of the security mechanisms of SCION and thus facilitated the development of improved variants of forwarding protocols that further strengthen security and achieve even better performance.

SCION Network



Attacker: controls subset of network (red)
Property: packets traverse authorized path. Rules out ineconomical paths, e.g., valley routing (yellow)

Research Highlights 2019

ZISC Welcomes the Applied Cryptography Research Group

The Applied Cryptography Research Group was established at ETH Computer Science in April 2019, under the leadership of Professor Kenny Paterson.

Cryptography provides a fundamental set of techniques that underpin secure systems. It includes basic techniques to enable services such as confidentiality and integrity of data in secure communication systems, as well as much more advanced methods such as cryptographic schemes that enable searches over encrypted data. It draws broadly from theoretical computer science (algorithms, complexity theory), mathematics (number theory, probability) and engineering (both electronic- and software-engineering).

Our research in Applied Cryptography brings all of these strands together to produce impactful **research that improves the security of today's and tomorrow's cryptographic systems.**

We work closely with industry to remediate any security issues that we find, following responsible disclosure processes. We are also working in standards bodies (IETF and IRTF) to lead the development of new cryptographic standards for the Internet.

Since its inception in the Spring, the group has grown to include 3 postdocs, 3 PhD students, and one long-term visitor.
Our 2019 research highlights include:

- Working with Florian Tramèr (visiting ETH Zurich from Stanford) and Dan Boneh (Stanford), we carried out an **analysis of two leading anonymous cryptocurrencies**, Zcash and Monero. We showed that both systems failed to achieve one of their main privacy goals, namely shielding the intended recipient of transactions from observers.

  We responsibly disclosed the vulnerabilities that we found in these systems to the Zcash and Monero teams, who were then able to patch the systems before any users were affected.

- Our **code-based post-quantum secure encryption scheme NTS-KEM** progressed to the second round of the NIST Post Quantum Cryptography process. We produced a security analysis of this scheme in the Quantum Random Oracle Model (QROM), giving greater assurance as to the soundness of the NTS-KEM design.

- We developed and analysed **a developer-friendly API for primality testing**. This API removes the need for developers to make complex, security-sensitive choices.

  It provides highly reliable results (false positive probability of 2^{-128}) in all use cases whilst

out-performing OpenSSL›s existing API in its default settings in typical use cases. We worked with the OpenSSL team to deploy this API in the OpenSSL crypto library. It will be included in the next major release of OpenSSL in Spring 2020.

- Our new postdoc Dr. Felix Günther won a prestigious **ACM SIGSAC Doctoral Dissertation Award** for his PhD thesis (from TU Darmstadt).

To read more about the group, please visit: https://appliedcrypto.ethz.ch/

Research Highlights 2019

Secure messaging: Stronger security with practical efficiency

Secure messaging (implemented for example in WhatsApp or Skype) allows a group of users to securely exchange private messages in a hostile (but nowadays the only realistic) environment, where the service providers try to intercept and inject messages, and where the endpoint mobile devices may get temporarily compromised (e.g. due to a virus) and leak their secrets.

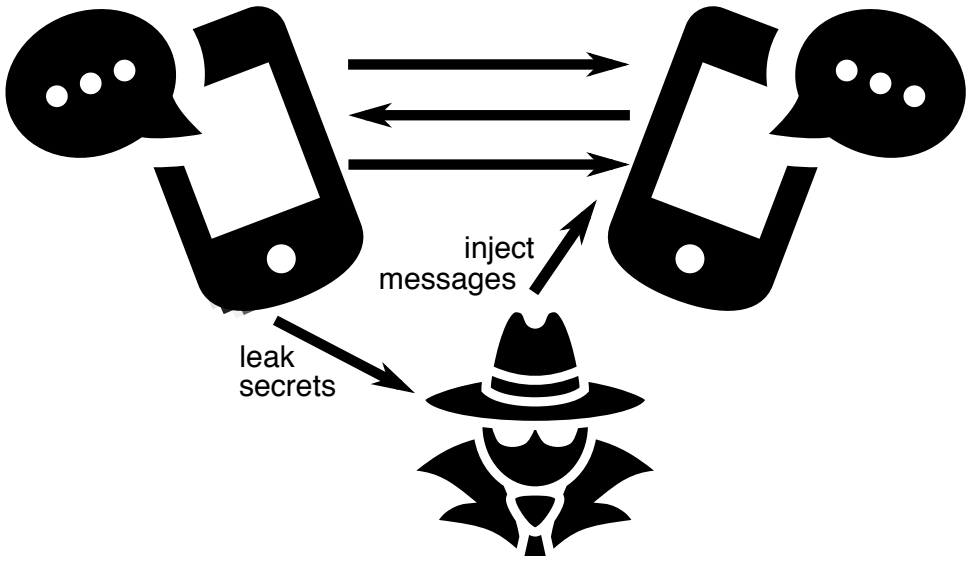
Surprisingly, **this setting still allows protocols with strong security guarantees.** For example, in case of two parties, Signal›s «double ratchet» algorithm (used by WhatsApp, Wire, Facebook Messanger and others) provides both **forward secrecy** (exposed secrets reveal no information about already received messages) and **post-compromise security** (confidentiality and integrity protection are restored after exchanging a few messages).

But even stronger security is possible. For example, since Signal uses symmetric primitives, exposing secrets of a user allows to read messages sent by her and inject messages to her. **This attack can be easily prevented by using standard asymmetric cryptography.**

However, even this is far from the best achievable security, recently characterized by the researchers. For instance, **the optimal guarantees imply a sort of man-in-the-middle-attack detection**: if an adversary uses exposed secrets of a user to inject a message to his partner, then the users can no longer communicate with each other (which hopefully allows them to realize they are under attack).
Unfortunately, the optimal security comes at a cost significant efficiency loss, caused by resorting to heavy non-standard cryptographic tools.

In a recent paper, we explore the trade-off between security and efficiency in more detail and present a protocol with security guarantees very close to optimal, but also with practical efficiency.

In particular, our protocol achieves all guarantees mentioned above, except in some rare situations. In the construction, we use cryptographic primitives with certain so-called key-homomorphic properties, which are provided by standard and efficient schemes (for example, the ElGamal encryption).



Education 2019

Security in School education

Center of Computer Science Education (ABZ) of ETH Zurich was founded with the goal to introduce computer science as a subject into school education. The main activities of ABZ include developing textbooks and online platforms for teaching computer science on all levels of schools and testing them in school, training teachers, popularization of computer science in the whole society, and supporting pupils for different CS competitions like Olympiad in Informatics, Informatics Beaver, ACM Programming Contests.

The main achievement is establishing "informatics" as a mandatory subject in Lehrplan 21 for obligatory schools as a result of long-term projects in more than 100 schools and more than 400 appearances in the media. The contribution to teaching "Security" include: Textbook "Einführung in die Kryptologie", several school projects on this topic and several courses for teachers for teaching cryptology.

The ZISC center is proud to support this project!

Main Research Areas

Smartphone Security

In this project, we focus on smartphone security. In particular, we look at how smartphones can enhance the security of our daily activities as well as how secure is data stored by users on smartphones.

Throughout our work we highlight the interaction of security with usability and deployability — two key components that cannot be ignored when designing and analyzing a secure system. We will see how in some cases decreasing or removing the user interaction requirements from a system render it more secure. In other cases, in contrast, it is the user interaction and attentiveness that play an important role in safekeeping. the data stored on a user's smartphone.

Monitoring

It is a growing concern for companies, administrations, and end users alike whether IT systems comply with policies regulating the usage of sensitive data. Checking compliance is particularly acute as our modern infrastructures (communication, entertainment, finance, etc.) collect, process, and share data.

A prominent approach to compliance checking is runtime monitoring. Here, system actions are observed and automatically checked for compliance against a given policy. We develop efficient and scalable monitoring algorithms for expressive policy specification languages, e.g., metric first-order temporal logic. We are also interested in policy enforcement, that is, preventing policy violations instead of only detecting them.

Future Internet Architecture SCION

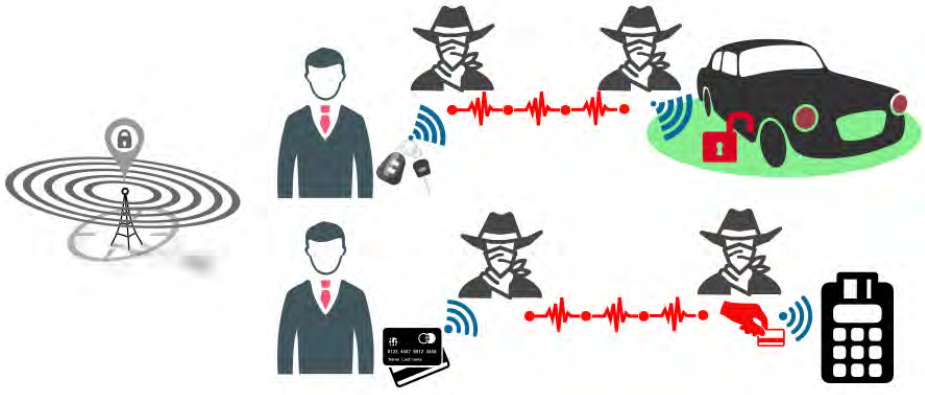
SCION is the first clean-slate Internet architecture designed to provide route control, failure isolation, and explicit trust information for end-to-end communications. SCION organizes existing ASes into groups of independent routing sub-planes, called isolation domains, which then interconnect to form complete routes. Isolation domains provide natural isolation of routing failures and human misconfiguration, give endpoints strong control for both inbound and outbound traffic, provide meaningful and enforceable trust, and enable scalable routing updates with high path freshness.

As a result, the SCION architecture provides strong resilience and security properties as an intrinsic consequence of good design principles, avoiding piecemeal add-on protocols as security patches.

Secure Positioning and Localization

In our daily lives, we increasingly rely on location and proximity measurements for important applications. Already today, people issue contactless payments simply by bringing their credit card close to a card reader. Modern cars automatically detect the key in proximity to unlock the doors. We see first instances of autonomous transportation drones navigate using GPS or Galileo.

The security of many existing and future applications surrounding navigation, access control, and secure routing critically depends on the correctness of the underlying location and proximity estimates.



Main Research Areas

Access control

Access control has wide range of applications, from physical access control, e.g., to buildings, over to access control in single applications, to enterprise-wide access control solutions for an entire company's data management.

Our work covers multiple facets of the challenges in effective access control. We work on languages for efficiently analyzable yet expressive access control policies, techniques for ensuring that no security-critical access control queries are omitted, mining access control policies, and modern systems for access control in physical systems.

Constructive Cryptography

Constructive cryptography is a new paradigm for defining the security of cryptographic schemes. It allows to take a new look at cryptography and the design of cryptographic protocols.

One can give explicit meaning to various types of game-based security notions of confidentiality, integrity, and malleability, one can design key agreement, secure communication, certification, and other protocols in a modular and composable manner, and one can separate the understanding of what cryptography achieves from the technical security definitions and proofs, which is useful for didactic purposes and protocol design.

Applied Cryptography

Cryptography provides a fundamental set of techniques that underpin secure systems. It includes basic techniques to enable services such as confidentiality and integrity of data in secure communication systems, as well as much more advanced methods such as cryptographic schemes that enable searches over encrypted data.

It draws broadly from theoretical computer science (algorithms, complexity theory), mathematics (number theory, probability) and engineering (both electronic- and software-engineering). Our research in Applied Cryptography brings all of these strands together to produce impactful research that improves the security of today's and tomorrow's cryptographic systems.

Security protocol verification

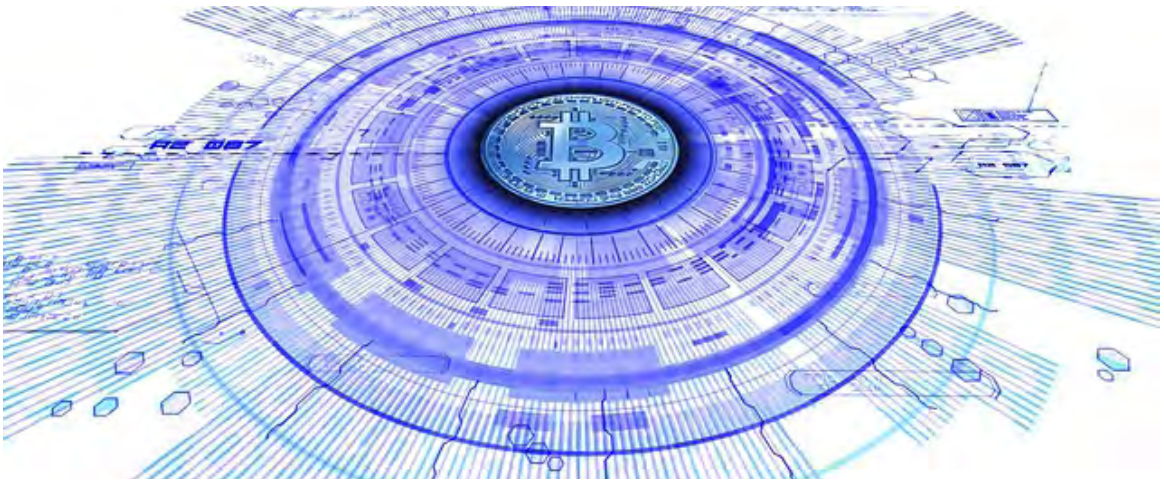
We develop tools for security protocol analysis in the symbolic model, particularly the Tamarin-prover. Security protocols are well-known to be error-prone, thus having a formal analysis enhances trust in the protocol's correctness. Our tools have theoretic foundations guaranteeing their conceptual correctness.

The symbolic model has a high level of abstraction compared to bitstrings over the wire, but provides automation and the ability to consider all modes of operation of a protocol at once. Practical results and impact has been seen in the standardization of TLS v1.3 and the analysis of the next-generation 5G mobile communication key exchange protocol 5G-AKA.

Blockchain Technology

Blockchain technologies promise many attractive advantages for digital currencies, financial applications and digital society in general. These advantages include reduced trust assumptions, increased transparency, reduced costs and improved user privacy. However, the current state-of-the-art solutions suffer from significant limitations.

In our research we investigate the limitations of current blockchain solutions and develop novel systems with improved security, privacy and performance guarantees. Examples of our research results include new types of smart contract execution environments, improved solutions for client privacy and novel digital currencies with regulatory support.



Research Projects

Highly Available Communication for Financial Networks

Communication, in particular for critical infrastructures, requires a high level of availability that remains available despite earthquakes, power outages, misconfigurations, or network attackers. One example is the financial industry, which has high requirements on availability to ensure that up-to-date trading information is accessible, that financial transactions are executed within short time windows, and that end customers can execute banking applications online.

The financial industry is generally a major target for network attackers, mainly because of the importance of availability for banking applications. The importance of availability has lead to several extortion attacks in the past, where banks would sometimes pay for attack termination in the short term, rather than protecting their networks for the long term.

To provide high availability and thus to make the financial industry robust against the aforementioned attacks and calamities, we investigate the deployment of multi-path connectivity between branches of one of our ZISC banking partners. In the context of the future Internet architecture SCION, designed and developed at ZISC, we focus on connecting branches over multiple existing links at the same time. We are deploying a multi-path communication system that automatically selects three, possibly independent, high-quality paths to avoid outages even if up to two of the independent paths fail.

To further increase the resilience against attacks, in particular in the context of DDoS defense and IoT security, our architecture offers the option to hide paths from the public and thus to prevent attackers from flooding such invisible paths. Moreover, we have developed a scalable bandwidth-reservation scheme that protects inter-domain communication by establishing fine-grained resource allocations to ensure no links between networks are saturated.

Publications

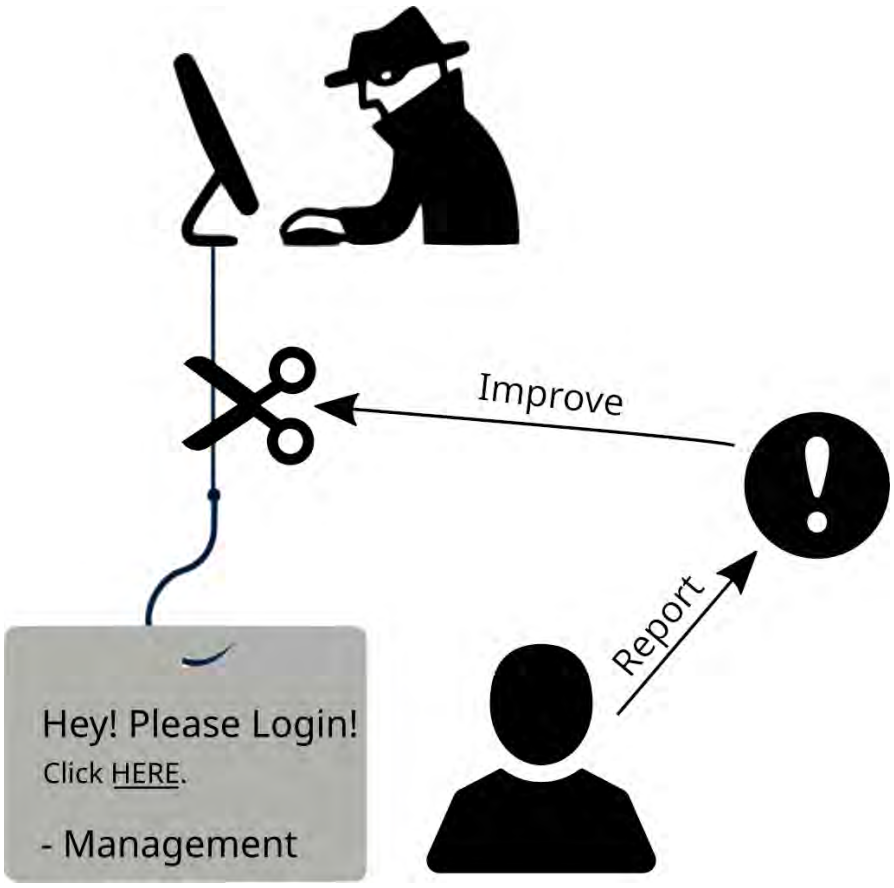
A. Perrig, P. Szalachowski, R. M. Reischuk, L. Chuat.
SCION: A Secure Internet Architecture
Springer International Publishing AG, 2017.

D. Barrera, R. M. Reischuk, P. Szalachowski, A. Perrig.
An Internet Architecture for the 21st Century
Communications of the ACM (CACM), 2017.

User-Complemented Phishing Protection

Phishing emails are deceptive messages made for data stealing and malware propagation. In this type of attack, miscreants pose as legitimate organizations (e.g., banks and financial institutions, delivery companies, shopping websites), and send emails crafted to look like the impersonated organization's. These emails try to solicit a sense of urgency, by prompting the user to act swiftly, usually by clicking on a link to change a reportedly compromised password, log in to confirm or update personal data. Such links lead to deceptive websites that are copies of the legitimate ones and often include login pages to try and trick the user into submitting their credentials. Other means for the attack can be opening malicious attachments or drive-by downloads of malware.

Phishing is a real threat to corporations: employees falling for phishing and revealing corporate credentials can be the first step for further attacks and data breaches. Phishing leads to significant economic losses: estimates put the yearly cost of phishing attacks for companies that fall victim in the order of million dollars. For this reason, it is of paramount importance to understand the most effective ways to protect users from phishing attacks.



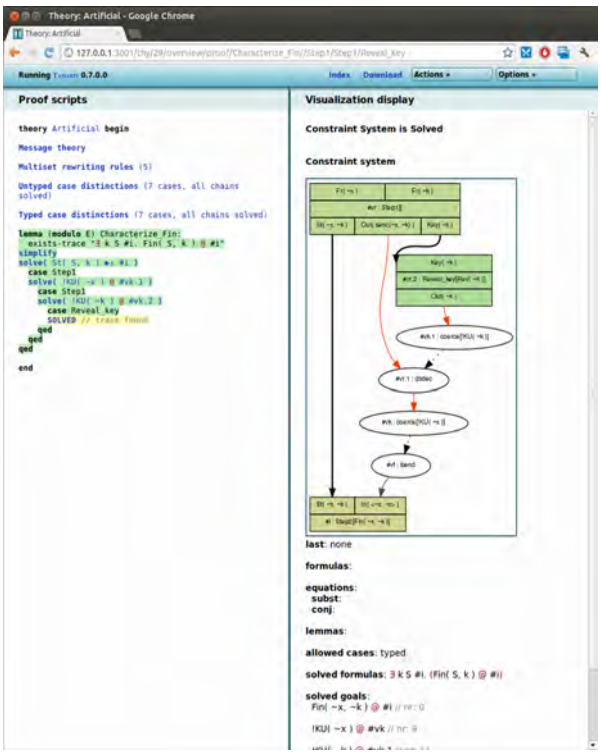
In this project, in partnership with the Swiss Post, we aim to conduct a large-scale study on phishing prevention, detection, and education. Users will be involved in phishing detection, by having the ability to report suspicious emails and to get feedback by automated analyses and human analysts after their reports. The project aims to find the best ways of involving users in a way that at the same time trains them to recognize phishing emails better. Moreover, we will analyze if user reports can be a useful first line of defense against 0-day phishing, by using reports to train machine learning classifiers that generate rules, instead of relying on burdensome manual creation by human experts.

Industry partner

Swiss Post

Research Projects

Formal Methods for Federated Identity Management



The Internet provides access to an ever increasing number of services, many of which require its users to have an account with credentials. This is a considerable cognitive burden for users and leads to password reuse and other poor security practices. Federated identity management services offer a way out of this dilemma. Using federated identity management, a user just needs a single account that employs strong protection (e.g., a unique password and a second authentication factor) at an identity provider and can then log in to other services with this account. An example of a widely used protocol to provide such a single sign-on experience for the user is OpenID Connect, based on the OAuth 2.0 standard.

While these protocols offer many advantages, they also pose security and privacy risks. The protocol specifications are complex, encompassing different modes for different scenarios. Various attacks on the protocols have been found in the past, for which countermeasures have been introduced, further increasing complexity. Furthermore, there are privacy issues that have not been fixed due to a lack of secure and functional alternatives.

For example, in OpenID Connect, the identity provider learns to which services the user logs in, and the exact time and frequency of these logins. In light of the General Data Protection Regulation (GDPR), fixing such privacy issues should be considered a priority.

We formally model the protocols as well as desired security and privacy properties, and employ state-of-the-art verification tools. In this way, we find problems with existing protocols and design provably correct protocol improvements. These tools verify the protocols with respect to an unbounded number of participants and sessions, and can therefore provide stronger security and privacy guarantees than manual analysis.

We also model different aspects of a user's internet identity, which encompasses accounts on various websites. For example, a user can have accounts with multiple identity providers, which are then used to log in to different relying parties. To obtain a more comprehensive analysis, we consider a user's entire account setup. We model all of the user's accounts, credentials, devices, and their connections.

Industry partner

ZKB

Security of Avionics Communication Systems

Next-generation avionics communication systems were — in the majority — standardised several decades ago, when only the most apt attackers were able to even receive aircraft signals. Therefore, security was not on the radar of the standardisation bodies who mainly focused on the safety impact of these protocols. This mismatch between safety and security led to systems that would keep the aircraft operating in a safe manner, even if individual systems failed.

Additionally, military and commercial (e.g. Amazon, Swiss Post) drones will in the intermediate future coexist with civilian aircraft in public airspace. This coexistence requires unmanned aerial vehicles (UAVs) to handle civilian aircraft communication in addition to the communication channels that control the drone.

This forest of communication system is a possible target for manipulation, eavesdropping and more advanced attacks. Any manipulation of the individual systems might lead to unforeseen consequences, as human intervention might be inhibited by an attacker.

In this project, we investigate the security of many different (mostly wireless) communication protocols. We will examine novel attacks against GPS technology and also take a look at the Traffic Alert and Collision Avoidance System (TCAS) employed by civilian aircraft and future drone systems. Further, we want to review satellite communication which serves as a backbone for medium and large sized drone systems as well as a multitude of commercial aircraft.

The target of this project is to research the security and privacy of today's aircraft and UAV communication systems and, where possible and applicable, propose changes to ensure the safety and security of tomorrow's flight operations.

Industry partner

Armasuisse

Research Projects

Blockchain and Cloud Security

In this project, NEC and ETH aim at addressing various issues in cloud and blockchain security in an aim to improve their security and scalability.

In the area of blockchain technology, our project focuses on the security and privacy of different blockchain technologies and on the development of new protocols and systems to enhance functionality.

First, we show that current scalability measures adopted by Bitcoin come at odds with the security of the system. More specifically, we show that an adversary can exploit these measures in order to effectively delay the propagation of transactions and blocks to specific nodes—without causing a network partitioning in the system. This allows the adversary to easily mount Denial-of-Service attacks, considerably increase its mining advantage in the network, and double-spend transactions in spite of the current countermeasures adopted by Bitcoin. Based on our results, we propose a number of countermeasures in order to enhance the security of Bitcoin without deteriorating its scalability.

Second, we propose a new approach to protect the privacy of lightweight clients in blockchain systems like Bitcoin. Our main idea is to leverage commonly available trusted execution capabilities, such as SGX enclaves. We design and implement a system called BITE where enclaves on full nodes serve privacy-preserving requests from lightweight clients. As we will show, naive serving of client requests from within SGX enclaves still leaks user information. BITE therefore integrates several privacy preservation measures that address external leakage as well as SGX side-channels. We show that the resulting solution provides strong privacy protection and at the same time improves the performance of current lightweight clients.

In the area of cloud security, our project investigated secure data deduplication and novel access control paradigms in the cloud. Deduplication allows storage reduction and makes cloud storage financially attractive to customers, but also generates numerous privacy and security challenges. Moreover, although the cloud encourages data sharing, existing access control paradigms do not fit all the new requirements arising from shared storage between partially-trusted partners. Therefore, in this project, we devised novel access control paradigms that allow data sharing according to users' needs.

Publications

S. Matetic, K. Wüst, M. Schneider, K. Kostiainen, G. Karame, S. Capkun
BITE: Bitcoin Lightweight Client Privacy using Trusted Execution
USENIX Security Symposium 2019

Industry partner
NEC

Towards Provably Secure Internet Communication

Nowadays, the wide-spread access to the Internet enables quick communication, unrestrained by physical location. However, this comes at a cost of new security risks, since now private messages become available to adversarial entities, located anywhere around the world. Hence, cryptographic protocols that add security to the communication become essential.

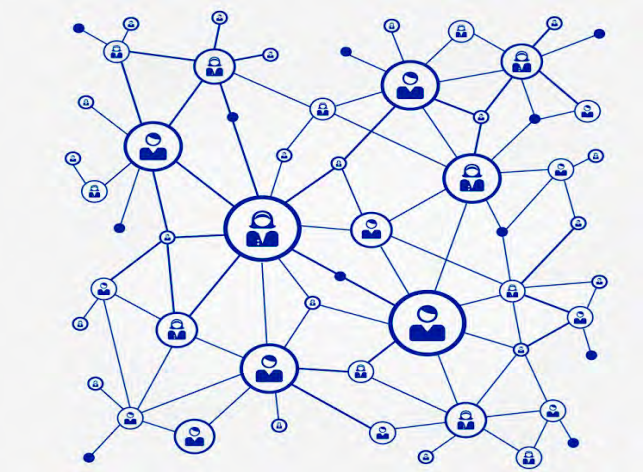
Since different situations have different functional and security requirements, the number of secure-communication protocols with different security-functionality-efficiency trade-offs is rapidly growing. For example, we have various session-establishment protocols (such as TCP-based TLS, or Google's QUIC based on faster but less reliable UDP), various secure-messaging protocols (such as Signal's double ratchet, or the group messaging protocol currently being standardized by the MLS working group), and many more. The large number of use cases, trade-offs and accompanying protocols (often designed in an ad-hoc fashion and without clearly specified security guarantees) motivates the goal of this project, which is to explore from the cryptographic perspective the space of secure-communication protocols.

More specifically, for various functionality requirements, we specify different security guarantees, where usually stronger guarantees require less efficient protocols. This is done with the help of cryptographic modeling tools, such as the (standard) game-based security analysis and the constructive cryptography framework (which, in particular, allows to express the strong guarantee of composability, i.e. a protocol is secure even if arbitrary other protocols are executed simultaneously).

This allows to, first, express the exact guarantees of existing protocols (and either verify that they meet their intuitive goals, or discover a gap between the intuition and reality) and, second, provide new protocols offering previously unexplored trade-offs.

Research Projects

Topology-Hiding Computation



Secure communication over an insecure network is one of the fundamental goals of cryptography. The security goal can be to hide different aspects of the communication, ranging from the content (secrecy), the participants' identity (anonymity), the existence of communication (steganography), to hiding the topology of the underlying network in case it is not complete.

Incomplete networks arise in many contexts, such as social networks, the Internet of Things (IoT) or ad-hoc vehicular networks. Hiding the topology can, for example, be important because the position of a node within the network depends on the node's location. This could in turn leak information about the node's identity or other confidential parameters.

Incomplete networks have been studied in the context of communication security, referred to as secure message transmission, where the goal is to enable communication between any pair of entities, despite an incomplete communication graph. Also, anonymous communication has been studied extensively. Unfortunately, none of these approaches can be used to hide the network topology. In fact, secure message transmission protocols assume (for their execution) that the network graph is public knowledge.

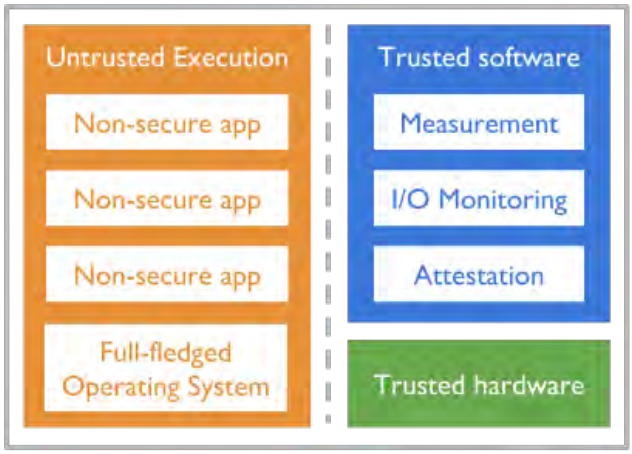
The goal of this project is to design topology-hiding communication protocols, which allow a set of parties connected by an incomplete network with unknown communication graph, where each party only knows its neighbors, to communicate in such a way that the network topology remains hidden even from a powerful adversary who can corrupt parties. These communication protocols can then be used to perform arbitrary tasks, for example secure multi-party computation, in a topology-hiding manner. In the formal analysis, we consider different degrees of network hiding. For example, a network may be completely hidden, or some partial knowledge about it may leak to the adversary. Recent results show that we can hide the topology up to leaking 1 bit of information about it with probability p.

Publications

Martin Hirt, Ueli Maurer, Daniel Tschudi, and Vassilis Zikas
Network-Hiding Communication and Applications to Multi-Party Protocols
Advances in Cryptology – CRYPTO 2016, Security and Cryptology, Springer-Verlag Berlin Heidelberg, vol. 9814, pp. 335-365, Aug 2016.

Rio Lavigne and Chen-Da Liu-Zhang and Ueli Maurer and Tal Moran and Marta Mularczyk and Daniel Tschudi
Topology-Hiding Computation Beyond Semi-Honest Adversaries
Cryptology ePrint Archive – 2018

Critical Infrastructure Security



The Internet of things (IoT) describes a plethora of embedded devices which are being built with increasing intelligence (programmability and computational power), and with network connectivity. These devices range from smart light bulbs and door locks in homes to automation and sensing in industrial, healthcare, and military settings. In all these scenarios, the promise of IoT is to enable a large number of new applications, a design space that is being aggressively explored by many platform manufacturers and software development companies.

However, IoT also represents a security hazard, due to a lack of proper security engineering in the race to claim fractions of the IoT market segments, and due to inherent challenges such as the dishomogeneity of platforms and operating systems, and the difficulty of keeping deployed devices up to date. One way of improving the security of these IoT devices is through relatively simple yet powerful security primitives embedded in standardized hardware components. These components, together with minimal verified software, can be used as a foundation on which trust in the entire device can be established. An example of this are the Security Extensions of Arm's embedded architectures, which provide a hardware-isolated environment in which trusted software (e.g., a verified micro-kernel) can be run to secure core functionalities such as security updates, sensitive cryptographic operations, and software measurement primitives which can be used to verify the rest of the software running on the device.

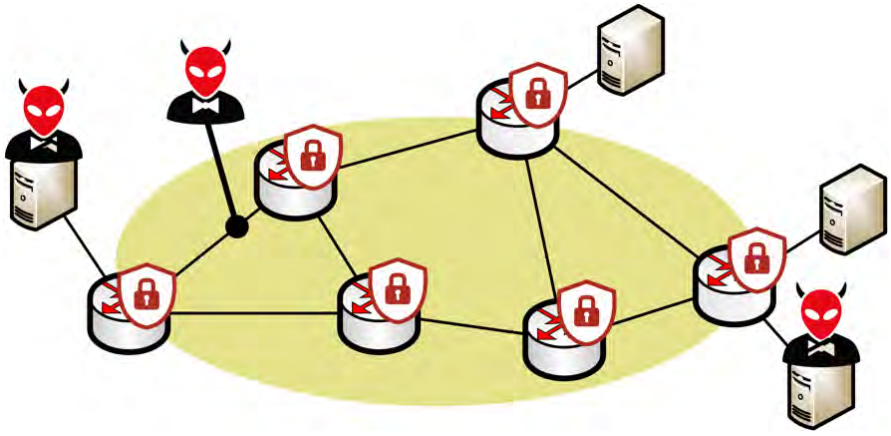
More recently, Arm has launched its Platform Security Architecture (PSA) framework, which aims to extend the security functionalities provided by the trusted environments. In this project we plan to investigate how these hardware components and architectures may be used to build powerful software tools for monitoring, enforcement, and recovery on IoT devices, focusing in particular on the most critical IoT use cases in the domains of industry, healthcare and military. Furthermore, through this work we aim to gain a better understanding in more theoretical terms of what types of high-level security primitives can be constructed from a minimal set of hardware-provided functionalities.

Industry partner

NEC

Research Projects

Improving Network Security Through Programmability



In this project, we argue that the network itself should be able to detect and mitigate attacks instead of relying purely on perimeter-based protection provided by dedicated appliances. To do so, we plan to leverage recent advances in network programmability which enable both the control plane and the data plane to be reprogrammed on-the-fly.

The goal of this project is to leverage recent advances in network programmability to make the network able to defend itself against: (i) anonymity and privacy attacks, performed by attackers which can eavesdrop on and modify traffic; and (ii) more general attacks (e.g., denial-of-service, data exfiltration), performed by attackers sitting at the edge of the network, on compromised hosts.

Protecting networks from in-network attackers. This part of the project aims at designing and developing a network-based anonymity and privacy framework targeted specifically at enterprise networks. Being network-based, the framework will enable to secure any connected devices (even unforeseen ones) and internal communications, without complex setup. To develop this "securing" network, we will actively leverage the new programmability primitives offered by Software-Defined Networks (SDN) in both the control plane (OpenFlow) and the data plane (P4).

Protecting networks from edge attackers. In this part of the project, we focus on attackers that get access to the network via one or more infected hosts. After infecting at least one host, such attackers usually initiate a "reconnaissance" phase in which they scan the network in search of high value targets. Network programmability enables to efficiently distribute the task of scan detection on the network devices and provides the ability to source traffic on the network device in order to implement advanced deception techniques in which the attacker is presented with fake information (e.g., fake IP addresses).

Publications

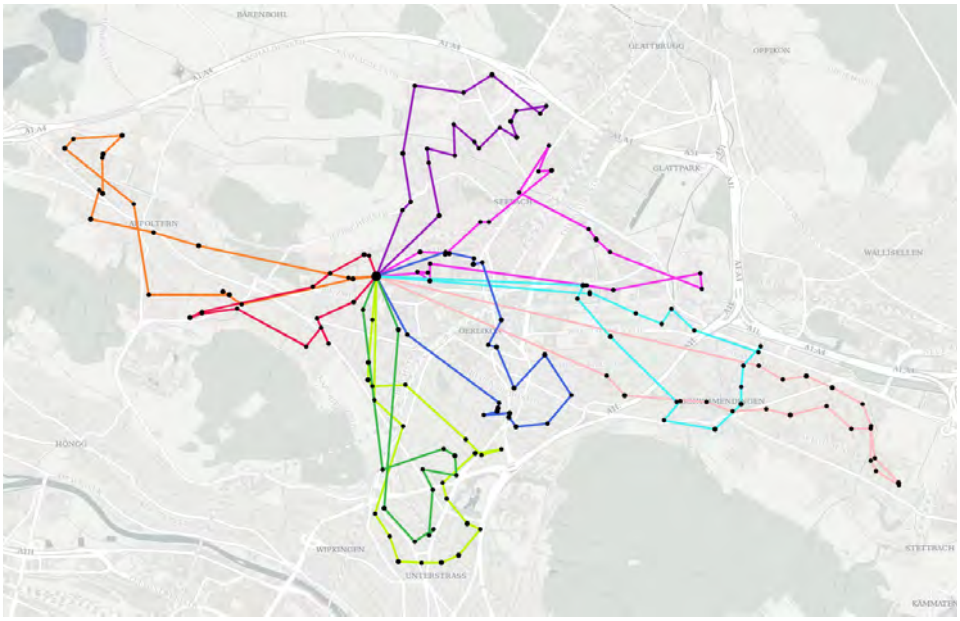
Roland Meier, Petar Tsankov, Vincent Lenders, Laurent Vanbever, Martin Vechev
NetHide: Secure and Practical Network Topology Obfuscation
USENIX Security 2018. Baltimore, MD, USA (August 2018).
For more details, see: https://nethide.ethz.ch

Roland Meier, Thomas Holterbach, Stephan Keck, Matthias Stähli, Vincent Lenders, Ankit Singla, Laurent Vanbever
(Self) Driving Under the Influence: Intoxicating Adversarial Network Inputs
ACM HotNets 2019. Princeton, NJ, USA (November 2019).
For more details, see: https://nsg.ee.ethz.ch/home/

New Routing Approaches for Bike Deliveries

In this project, ETH and the Swiss Post/notime AG aim at addressing novel challenges appearing in routing problems for same day deliveries.

The business to customer delivery market has experienced significant changes in recent years. In particular, regarding parcel logistics, same day delivery has become a major component, enjoying continuously increasing demand and generating extensive extra efforts for delivery companies in solving challenges that come along with this growth. A key aspect among these challenges that is of particular importance for same day deliveries is the last mile, where parcels have to be distributed from a depot to customer addresses in the same city within a short time window. The last mile in same day deliveries is often done by bike couriers, which are faster and more flexible in urban areas compared to delivery trucks. Typically, a bike courier loads his cargo bike at the depot once or twice during one delivery time window, and follows a pre-computed delivery route that is provided to him.



From an algorithmic point of view, both the tasks of assigning parcels to bike couriers on the one hand, and defining strong and on-time delivery routes on the other, are highly nontrivial. Needless to say, the two questions are highly dependent, thus forcing a global approach in order to obtain solutions of good overall quality. An additional challenge stems from the need to support unforeseen real-world changes in the problem instance, like potential delays on some of the routes or new/cancelled orders, that have to be anticipated on short notice. These aspects of the problem require the design of very fast routing algorithms that can be run many times during the same day to be able to react to changes and revise decisions taken earlier.

Our goal is to leverage modern techniques from Combinatorial Optimization to design fast routing algorithms addressing the challenges sketched above that return solutions for which we can provide strong guarantees in terms of solution quality.

Industry partner

Swiss Post / notime AG

Research Projects

Full-Stack Verification of Secure Inter-Domain Routing Protocols

Inter-domain routing is a part of the Internet's core infrastructure. Despite its important role, the currently most widely deployed Border Gateway Protocol (BGP) allows for, and has been observed to suffer from, attacks leading to severe disruptions of the Internet. While there have been proposals for more secure variants of BGP, these protocols come with performance penalties and provide protection only against certain attacks.

This prompted the development of SCION (Scalability, Control and Isolation on Next-Generation Networks). SCION is a clean-slate Internet architecture that provides secure routing and packet forwarding, alongside a number of other desirable properties.

In this research project, we examine the SCION protocols in detail and formally verify that they have the desired security properties. We first formalize the protocols and security guarantees, and then use techniques from refinement and interactive theorem proving for their verification. Finally, we extract from the proven assertions a low-level specification of the IO-behavior of SCION components.

We then use this specification to formally verify the Python and Go implementations of the SCION routers. In particular, we prove the absence of runtime errors and the implementation's compliance with the specification, i.e., its functional correctness. Additionally, we prove security-related properties of the implementation like secure information flow.

Since the verification effort on the protocol level uses a different formalism than the verification of the code level, a sound link has to be created between them. We realize this link by a refinement step that translates the abstract model into a specification of its IO-behavior. The soundness of this translation is proved in an interactive theorem prover.

Our goal is to gain a better understanding of the underlying properties of the SCION protocol and routing protocols in general, and to improve on the state of the art for the verification of concurrent, object-oriented programs. Moreover, this work will contribute to the first Internet protocol suite that has been verified from the ground up.

Publications

Marco Eilers and Peter Müller and Samuel Hitz
Modular Product Programs
European Symposium on Programming (ESOP), 2018.

Marco Eilers and Peter Müller
Nagini: A Static Verifier for Python
Computer Aided Verification (CAV), 2018.

Quantum players in constructive cryptography

Quantum mechanics is one of the most successful physical theories, and has been verified by numerous experiments. But what does this imply for cryptography? On one hand, adversaries may have abilities that are not captured by a "classical" adversary. On the other, the (honest) users may also use quantum technology to increase the security of their protocols. But before being able to formulate the risks and benefits of quantum players, one needs cryptographic models and security definitions that encompass such parties.

The goal of this project is to model quantum players in the constructive cryptography framework of Maurer and Renner. The first part of the project involves modifying the framework itself so that it has the power need to capture such quantum players. For example, quantum mechanics allows a message to be in a superposition of sent and not sent, or a superposition of sent to Alice and sent to Bob, which needs to fit in the underlying communication model used by the framework. Furthermore, one may consider various message scheduling models, e.g., sequential scheduling (the players are activated one after the other), time-based scheduling (the time it takes to send and receive messages is explicitly modeled, and used to determine the order in which messages are processed) and non-determiistic scheduling (one computes all possible orders of messages and looks at the worst case). This projects studies these different scheduling models in the quantum context.

The second part of the project consists in using the framework to model cryptographic security in various applications. For example, we wish to find the best way to model CPA and CCA attacks on schemes that encrypt quantum messages. Another example is to study device-independent cryptography, and model the reuse of devices in a composable framework. It is indeed well-known that current security proofs only hold for devices that are used just once.

Publications

Fabio Banfi, Ueli Maurer, Christopher Portmann, Jiamin Zhu.
Composable and Finite Computational Security of Quantum Message Transmission.
To appear at TCC 2019.

Christopher Portmann
Quantum Authentication with Key Recycling.
Advances in Cryptology – EUROCRYPT 2017 – Proceedings, Part III, pp. 339-368, 2017.

Research Projects

Robotic stacking of parcels in containers and roll cages

Problem statement: The employees of Swiss Post do a great amount of manual work to load and unload parcels in containers. The unloading process can be automated mechanically (e.g. by tilting the roll cages), but an acceptable level of filling by the loading process cannot be achieved through a mechanical solution: parcels must be intelligently stacked in order to optimize the volume transported.
A robot could do this work, but the current technologies are based on a process in which every item to stack is known in advance. In the postal industry, it is impossible to know which item is coming next, although some properties of each item are known (e.g. size and weight). This project will focus on the development of an intelligent robotic system capable of loading containers and roll cages using low to no buffer.

Basic research: Solving the problem stated above requires intelligent robots that know how to dynamically manipulate rigid boxes. This task requires specialized motion planning algorithms for 1) robust grasping and 2) collision-free trajectories to efficiently move boxes from the conveyor belt to their final location in the container.

Both sub-tasks must take into account the workspace of the robot. For example, if reachability is somewhat limited, then the boxes could be tossed gently, or placed down and pushed into their final spot. Such strategies, which are often employed by human workers, require robots to poses a deep understanding of contacts and friction, dynamics, robustness against unanticipated perturbations, dynamic regrasping strategies, etc. The ultimate goal of this PhD thesis is to endow robots with human-level skill when it comes to loading parcels.

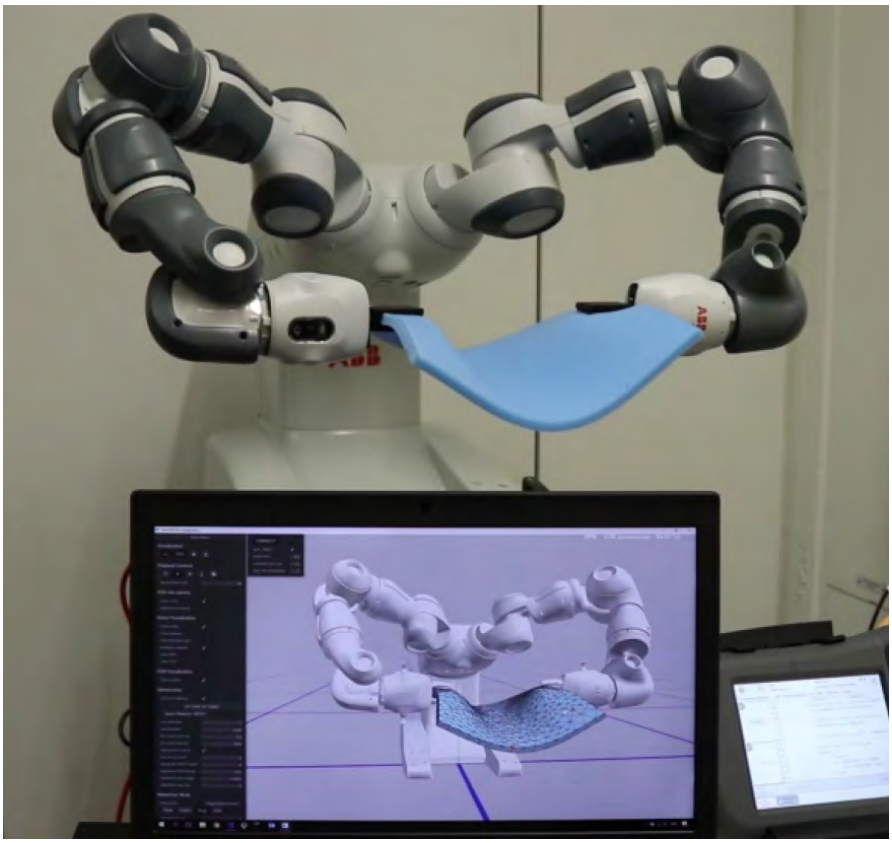
Technical foundations that the CRL group will contribute to:

1. Physics-based simulation models that will let robots understand and predict the physical implication of their actions.

2. A differentiable simulator as the technical foundation for trajectory optimization algorithms that will generate dynamic motion plans.

3. Robotic tele-operation as the means to learn complex motion skills from demonstrations.

Manipulation of non-rigid e-commerce parcels



Problem statement: The Swiss Post knows how to process form-stable items (Letters or packages). For these types of items, we have appropriate technologies. With the growing volume of e-commerce items from Asia, however, we have the challenge that the range (material, size, unstable structure, surface pressure, different shapes ...) of these items vary massively.

For this spectrum, we do not yet have suitable technologies in the postal industry. Therefore, the decision for the subsequent process is made by a manual (feel with the hand) and visual judgment by the employee. They touch, turn, look, bend the item.

Basic research: Solving the problem stated above requires robots that can dexterously manipulate soft, unstructured parcels and polybags. To this end, we will build on the model-based methodology my research group has recently introduced.

In particular, the goal of this thesis will be to develop technical foundations to allow the robot 1) to build an internal mechanical model of soft/unstructured parcels by feeling/scanning/manipulating the items, and 2), to autonomously understand how to grasp, pick up, and dynamically place the soft parcel on a conveyer belt in a prescribed configuration.

Technical foundations that the CRL group will contribute to:

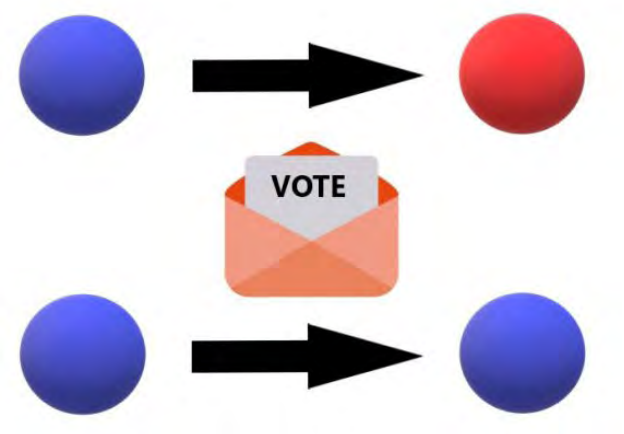
1. Physics-based simulation models that will let robots understand and predict the physical implication of their actions.

2. A differentiable simulator as the technical foundation for trajectory optimization algorithms that will generate dynamic motion plans.

3. Robotic teleoperation as the means to learn complex motion skills from demonstrations.

Research Projects

Secure Governance Schemes for Blockchains



Systems based on blockchain technology are promising, as they can be decentralized and rendered robust against attacks. A blockchain is a (distributed) ledger, in which all transactions are recorded sequentially. Because such systems build on distributed consensus –i.e. they require a large number of participants to agree on whether a new transaction should be valid, which they do by holding a copy of the ledger– they function without the need to build trust among its participants or to rely on a trusted third-party.

A blockchain is also governed by a number of parameters such as the block size, the upgrade specifications or the reward systems for validators. Following the decentralization principle underlying distributed consensus, it should be possible for all blockchain stakeholders to have a say on changing these parameters, i.e. to decide about the governance of the blockchain. Yet, most blockchains exclude the majority of stakeholders (participants) from governance.

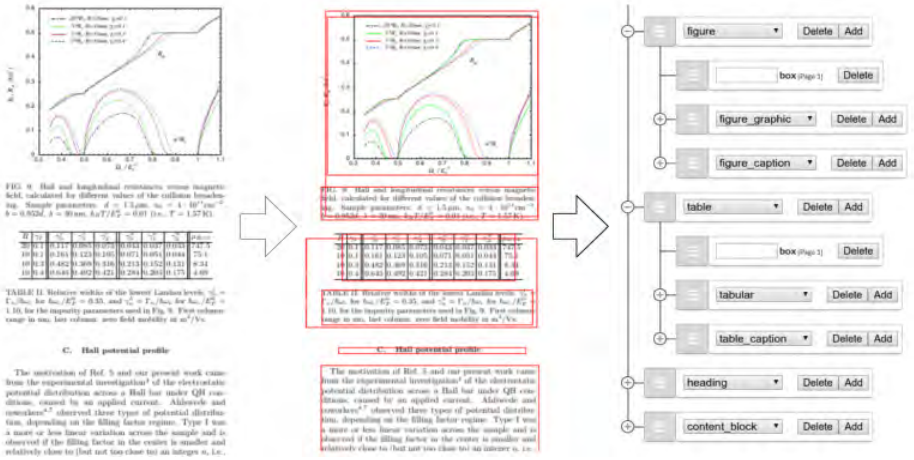
We develop a new secure voting scheme for the governance of a proof-of-stake blockchain, which we generically call Blockchain Assessment Voting (BAV). Although our focus is on governance, we also expect to reap insights that can be helpful to achieve distributed consensus more efficiently.

BAV schemes consist of two voting rounds. When a proposal is made, some randomly selected stakeholders obtain voting rights in relation to their stakes, but their anonymity is preserved. These stakeholders (simultaneously) vote on the proposal on the table, which is pitted against the status quo. The result of this first voting round is observed by all stakeholders, no matter whether they participated in the first round or not. Upon publication of the first-round results, the proposal may be retracted or amended by its authors, in which case BAV stops.

Alternatively, BAV may also stop if some pre-determined vote threshold has not been reached in this first voting round. If it has not stopped, the scheme continues with the second stage, in which the proposal is put to vote among the remaining stakeholders. The final decision between the proposal and the status quo is taken by adding the votes of the two voting rounds.

In the context of blockchains, one might also want to allow stakeholders to delegate their voting rights to other participants, but this could open possibilities for manipulation. We will use mathematical tools and a blockchain architecture based on proof-of-stake to assess whether and how BAV schemes could be used to improve outcomes in blockchain decisions and how they could prevent manipulation of outcomes by a small coalition.

Automatic Visual Document Parsing



Automatic information retrieval methods are powerful tools to build structured knowledge bases from large datasets of real-world documents in science, industry and the public sector. The system we are building automatically produces an intermediate representation for a diverse range of documents that can be used by such information retrieval methods. It takes as input PDF documents or document images and translates them into JSON files containing the natural semantic hierarchy representing a document. These JSON files can be queried using a document database, and be used as a uniform document representation by downstream information extraction engines.

A major obstacle in using information retrieval methods on documents in PDF format is the lack of machine-readable structure information, e.g. document sections, tabular contents, lists, etc. Due to this challenge, ad-hoc code typically has to be written to correctly extract document contents for differently formatted documents. This approach often fails to generalize over varying document formats and code has to be re-written to cope with even minor format changes.

Instead of manually extracting contents from PDF raw data, we leverage the visual document representation for more robust content retrieval, similar to how a human reader would process the information. A convolutional neural network that operates on the rendered PDF documents is applied in our system. The network is trained for the task of page entity detection, e.g. the prediction of the locations of figures, tables and contained table cells and captions.

We pretrain the neural network in a weakly-supervised fashion on a large dataset of annotated documents that was automatically created from publicly available scientific articles. This weak supervision strategy greatly reduces need for manual annotation and allows for efficient adaptation of our system to new document types. In a subsequent step, structural relationships between detected page entities are automatically identified in order to produce the full hierarchical structure for document pages.

Industry partner

Zurich

Further Information

For more information:
https://zisc.ethz.ch/

How to find us:

Postal address

ETH Zurich
Department of Computer Science
Zurich Information Security and Privacy Center
Universitätstrasse 6
CAB/CNB F
8092 Zurich

Physical address

Entrance to CNB building

ETH Zurich
Department of Computer Science
Zurich Information Security and Privacy Center
Unversitätstrasse 6
Buildings CNB and CAB, floor F (ZISC OpenLab F100.9)
8006 Zurich
Schweiz

phone +41 (0)44 632 72 43
fax +41 (0)44 632 11 72

People

ETH Faculty in ZISC
The ZISC center includes the following ETH faculty members:

Prof. Dr. David Basin, leads the Information Security Group that performs research on methods and tools for the analysis and construction of safe and secure systems.

Prof. Dr. Srdjan Capkun (ZISC director) leads the System Security Group, studying the design and the analysis of security protocols for wired and wireless networks and systems.

Prof. Dr. Ueli Maurer leads the Information Security and Cryptography Group that focuses on information security, theory and application of cryptography and theoretical computer science.

Prof. Dr. Kenneth Paterson leads the Applied Cryptography group. The group's research interests lie in all aspects of Cryptography, especially Applied Cryptography.

Prof. Dr. Adrian Perrig leads the Network Security Group whose research revolves around building secure and robust network systems – with a particular focus on the design of future Internet architectures.

Contact

https://zisc.ethz.ch/

ETH Zurich
Department of Computer Science
Zurich Information Security and Privacy Center
Universitätstrasse 6
CAB/CNB F
8092 Zurich
Schweiz