ETH zürich

Zurich Information Security and Privacy Center (ZISC)

Annual Review 2018

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 2018

During 2018, the ZISC center has carried out numerous research projects in cooperation with its partners. The topics of these projects include highly available communication for financial networks, formal methods for federated identity management, cloud and blockchain security, verification of routing protocols, phishing protection, provably secure Internet communication, topology-hiding computation, provably secure blockchains, automated document parsing and quantum cryptography.

The ZISC center has also organized several academic events and technical workshops. During 2018, more than 20 talks took place in our weekly series of technical talks, called the ZISC lunch seminar. The list of speakers included world-leading experts and researchers such as Prof. Bryan Parno from the Carnegie Mellon University, Ian Miers from Cornell Tech, and Pauline Anthonysamy and Bram Bonne from Google. In January, ZISC supported the Real World Crypto 2018 Symposium in Zurich. In June, ZISC organized a summer school on blockchains and real-world crypto at Sibenik, Croatia. In September, ZISC hosted a session on information security at the Digital Festival in Zurich. In addition, ZISC continued to support the ETH Studio initiative at New York City in collaboration with Cornell Tech.

Research Highlights 2018

ETH researchers uncover security gaps in the 5G mobile communication standard

Researchers in the Information Security Group subjected the upcoming 5G mobile communication standard to a comprehensive security analysis. Their conclusion: data protection is improved in comparison with the previous standards 3G and 4G. However, security gaps are still present.

Two-thirds of the world's population, about five billion people, use smartphones or other mobile devices on a daily basis. They connect to the mobile network via their SIM cards and make calls, send texts, swap pictures, or make payments and purchases. For mobile providers, the business is worth billions. But not just for them. Again and again, criminals have been able to access the communication between a device and a network in order to intercept conversations or steal data.

The fifth and newest mobile communication generation promises users significantly more security than before. In order to guarantee security, key factors must be considered: the device and network must be able to authenticate each other, and the confidentiality of the data exchange and the privacy of the user concerning identity and location must be guaranteed.

This has been implemented through a protocol known as Authentication and Key Agreement (AKA) since the introduction of the 3G standard. The organisation 3rd Generation Partnership Project (3GPP) is responsible for the specifications of this protocol, and for the specifications of the newest standard 5G AKA.

The 5G mobile communication standard does not close all gaps

A team of ETH researchers from the group headed by David Basin, Professor of Information Security, has now taken a closer look at these specifications. With the aid of the security protocol verification tool Tamarin, they systematically examined the 5G AKA protocol, taking the specified security aims into account. Tamarin was developed and improved during the last eight years in this research group and is one of the most effective tools for analyzing cryptographic protocols. The tool automatically identifies the minimum-security assumptions required in order to achieve the security objectives set by 3GPP.

> "It showed that the standard is insufficient to achieve all the critical security aims of the 5G AKA protocol,"

says senior scientist and co-author Ralf Sasse.

> "It is therefore possible for a poor implementation of the current standard to result in users being charged for the mobile phone usage of a third party."

Fault correction possible before the 5G launch

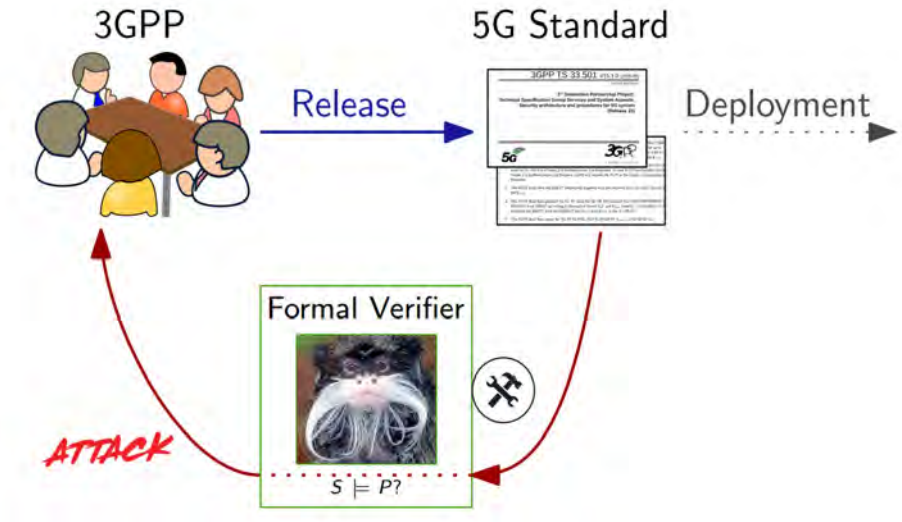
As Basin's team determined, data protection will be improved significantly with the new protocol in comparison with 3G and 4G technologies. In addition, 3GPP succeeded in closing a gap with the new standard that had previously been exploited by IMSI catchers. With these devices, the International Mobile Subscriber Identity (IMSI) of a mobile phone card can be read to determine the location of a mobile device. To achieve this, the device masquerades as a radio station in order not to be caught by the mobile phone.

> "This gap is closed with the 5G AKA. However, we have determined that the protocol permits other types of traceability attacks,"

explains senior scientist and co-author Lucca Hirschi. In these attacks, the mobile phone does not send the user's full identity to the tracking device, but still indicates the phone's presence in the immediate vicinity.

> "We assume that more sophisticated tracking devices could also be dangerous for 5G users in the future,"

adds Hirschi. If the new mobile communication technology is introduced with these specifications, it may lead to numerous cyber attacks. Basin's team is thus in contact with 3GPP, in order to jointly implement improvements in the 5G AKA protocol.



Research Highlights 2018

DelegaTEE: A new system that enables secure sharing of web service accesses amongst users

Delegation, the ability to share capabilities or privileges selectively to other entities, is a well-studied concept in access control. Delegation remains mostly unsupported in today›s online services, however. Most web-based financial services lack support for any kind of delegation, while other services, such as Facebook, support it in a limited and coarse-grained way. Facebook allows a user to delegate to a third-party application the authority to post to the user›s wall, but not to impose a limit of, say, three posts per day.

The ability to delegate access to existing online accounts and services, safely and selectively, could give rise to new forms of cooperation among users.

One example is flexible sharing (or resale) of digital content, such as streaming services like Netflix. Another is the outsourcing of online tasks, such as replying to email, to remote workers. Yet another is delegation of access to financial service accounts, such as Paypal. Given such capabilities, ordinary users could play a role in broadening global financial inclusion.

If users want to share data or delegate access to services in ways not natively supported by their service providers, they must resort to sharing credentials directly. This is a dangerous practice: an abused shared credit-card number can mean significant monetary loss, while an abused shared password can result in high charges, service termination, and even legal jeopardy. Such dangers naturally deter against many forms of online content and service sharing.

The goal of our work was to enable delegation by the entity that has access to a resource or a service (Owner), to a borrower (Delegatee) of that resource or service, while achieving several key properties. Delegation should be *fine-grained* to limit the capabilities of the Delegatee in carefully specified ways, and *trust-limited*: the Owner and Delegatee do not need to trust each other.

We refer to the new kind of flexible and powerful sharing of resources embodied in these properties as *brokered delegation*.

Brokered delegation has only recently become broadly practical thanks to recent advances in *trusted execution environments* (TEEs), a hardware-based application-security technology that is available today in Intel chipsets under the name Software Guard eXtensions (SGX) as well as the Keystone project in RISC-V based systems and ARM TrustZone.

To demonstrate the potential of brokered delegation for many existing web services, we developed DelegaTEE, and show several application prototypes that could give rise to new markets: outsourcing of personal/commercial microtasks, tokenization, resale of resources/services, and new payment methods.

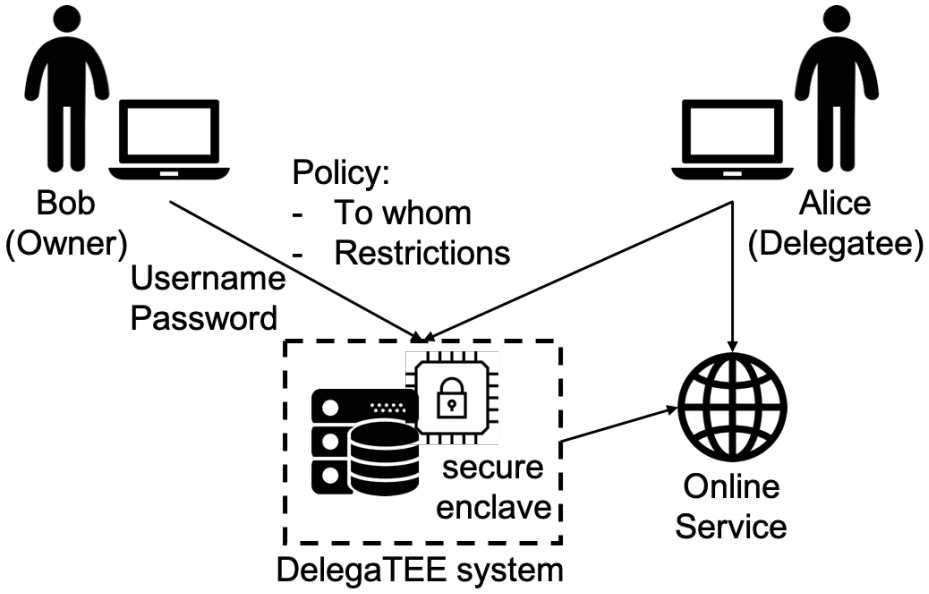
One of the key features of DelegaTEE is its high degree of provider-independence: *it requires no changes whatever to the service managing the resource or to users accounts*.

Depending on the application, DelegaTEE can either enrich a target service or undermine its security policies (or both). For example, reselling a paid subscription service in regions where the service is intentionally restricted undermines the services security

policy, while delegating access to office tools such as mail and calendar to administrative assistants can enrich the capabilities and usability of the service itself.

By enabling new forms of sharing and cooperation among users, DelegaTEE evokes the technology-fueled resource-sharing models for physical resources pioneered by Airbnb and Uber. These companies have challenged legal and regulatory frameworks while creating and delivering appealing new services.

We view DelegaTEE as a catalyst for a new class of such contributions to the sharing economy.



Research Highlights 2018

Secure distance estimation using cryptographic operations at the physical layer

Proximity and distance have so far been used in a number of security and safety-critical applications. Researchers have focused on designing the Challenge-Response approaches to make these systems secure. However, these systems are still vulnerable due to physical layer attacks.

In a typical access control environment, an authorized person simply taps his smart card against a card reader at the entry point to gain access to the infrastructure. For payments, the user can simply place the contactless card in close proximity (a few centimeters) to the payment terminal. Moreover, modern automobiles can use Passive Keyless Entry Systems (PKES) to unlock, lock or start the vehicle when the key fob is in close proximity to the vehicle, without taking out the key from the pocket.

Smartcard-based physical access control and authentication are deployed even in critical infrastructures such as nuclear power plants and defense research organizations.

In all the above systems, the entities send cryptographically-generated challenge bits and expect the correct response bits within a certain time window.

Previous researches have demonstrated that these systems are vulnerable to relay and other physical layer attacks - an external attacker can prove that the entities are closer even when they are farther apart. Most notable examples include relay attacks on passive entry/start systems in cars and credit card payments. Real-world instances of car theft have also been reported, such as hacking of Tesla's keyless entry system. Video footage of thieves relaying signal from a key inside a home to unlock a car in the driveway has gained widespread media attention. These instances show that the cryptographic generation of bits does not prevent physical layer attacks.

The only system secure against the attacks mentioned above is the Ultra-Wideband Impulse Radio (UWB-IR) with a short symbol length, i.e., a single pulse to represent a bit.

To reduce the perceived distance between two entities, the attacker needs to learn the symbol structure of each bit. In a single-pulse-per-bit system, attacker needs to learn the structure of each pulse. The pulse length is too short (2ns), hence the attacker will be able to reduce distance by at most 1m. However, this system achieves security by sacrificing performance (i.e., limiting the maximum distance of measurement).

"The existing ranging system provide choice between longer distance or security."

Longer symbols with multiple pulses are performant, but vulnerable due to the predictable nature of the symbol structure - an attacker can learn the symbol structure by looking at a part of the symbol.

The team of ETH researchers from the group headed by Srdjan Capkun, Professor of System Security, has designed a technique to prevent these attacks.

The attack is prevented by making the symbol structure unpredictable for the attacker - the cryptographic operations are applied to pulses at the physical layer.

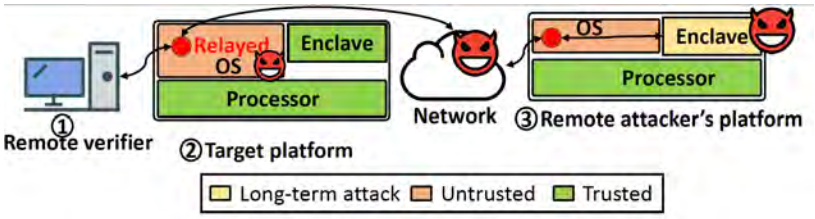
This technique achieves secure distance measurement between two mutually trusted devices against all physical-layer distance reduction attacks without sacrificing performance and simultaneously enabling extended range and security.

"The cryptographic operations at the physical layer of the ranging system enable secure ranging for the extended range."

Research Highlights 2018

Hardened SGX Attestation Using Proximity Verification

Modern applications are extremely diverse in nature and often users offload them to remote server. One such example is cloud computing platforms where the user uploads their sensitive data to execute some operation on them. The applications may handle sensitive data such as medical records, financial information, genetics data, etc. In such cases special protection is required to safeguard the data from an attacker who can compromise the operating system.



Intel, from their 6th generation processor family onwards, enables a feature named SGX or Software Guard Extension.

Intel SGX enables protected enclaves on untrusted computing platforms. SGX provides two powerful features: execution privacy and integrity.

Privacy is achieved by memory encryption where the protected application is encrypted on the memory that is hidden from the untrusted OS. The integrity is achieved by the attestation mechanism.

An important part of SGX is its remote attestation mechanism that allows a remote verifier to check that an enclave was correctly constructed before provisioning secrets to it.

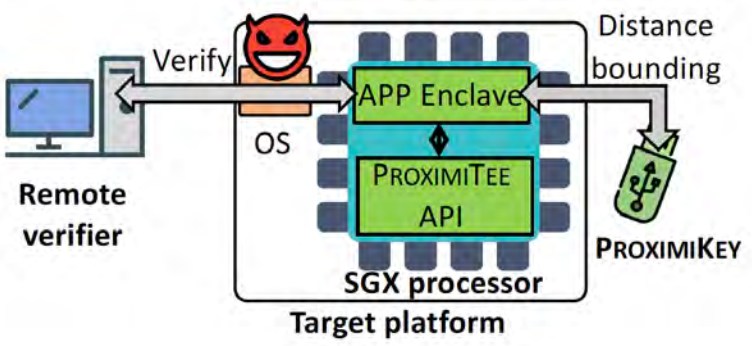
SGXs trust model assumes that the attacker can fully compromised the OS. Due to such attacker model, SGX attestation is vulnerable to relay attacks where the attacker, such as malicious OS, redirects the attestation and therefore the provisioning of confidential data to a platform that he physically controls. The implication of this attack could be devastating. Given this redirection, the attacker has unlimited time to mount side-channel, micro-architectural and physical attacks to compromise the enclave.

We propose ProximiTEE, a novel solution to prevent relay attacks. Our solution is based on a simple embedded device, and it is best suited to deployments where the deployment cost of such a device is minor compared to its security benefit.

During attestation, the embedded device that is attached to the target platform verifies the proximity of the attested enclave using distance bounding, thus allowing secure attestation regardless of a compromised OS.

The distance bounding relies on the fact that the channel between the target platform and the ProximiKey device is faster than the network interface between the target platform and the attackers platform. This allows the ProximiKey device to distinguish between communication with the legitimate enclave running on the physically connected platform and the attackers relayed data.

The device also performs periodic proximity verification which enables secure enclave revocation by simply detaching the device.



Main Research Areas

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.

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.

Smartphone Security

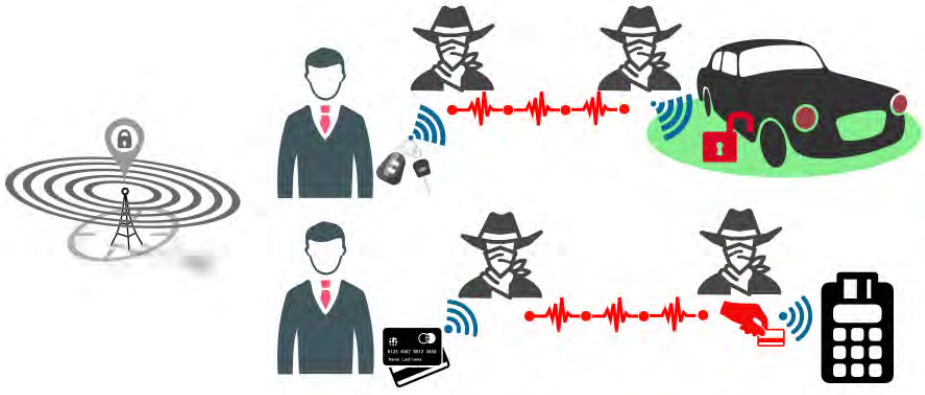
In this project, we focus on smartphone security. In particular, we look at how smartphones can enhance the security of our daily activities as well as how secure is data stored by users on smartphones.

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 safe-keeping. the data stored on a user's smartphone.

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.



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.

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.

Monitoring

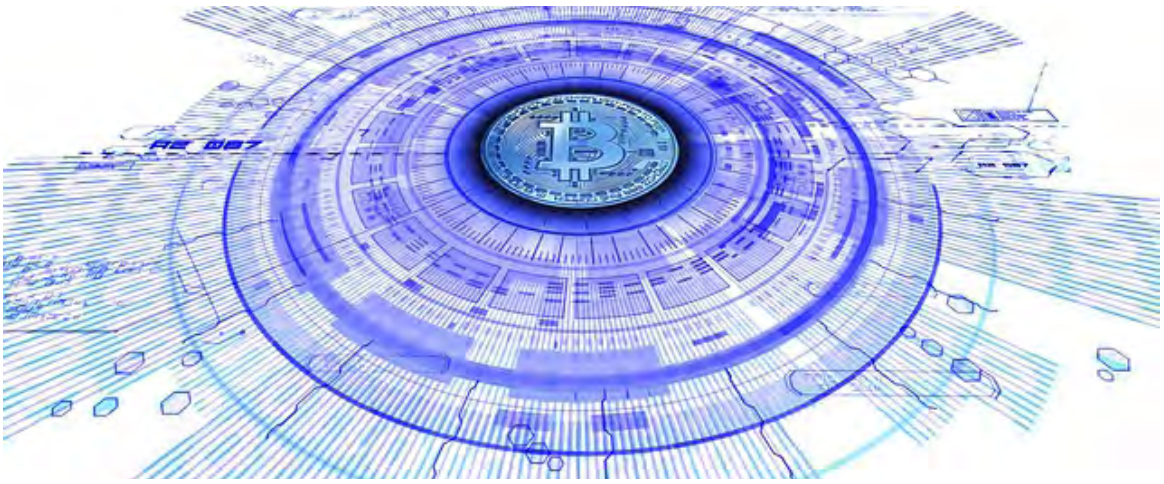
It is a growing concern for companies, administrations, and end users alike whether IT systems comply with policies regulating the usage of sensitive data. Checking compliance is particularly acute as our modern infrastructures (communication, entertainment, finance, etc.) collect, process, and share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

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.



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.

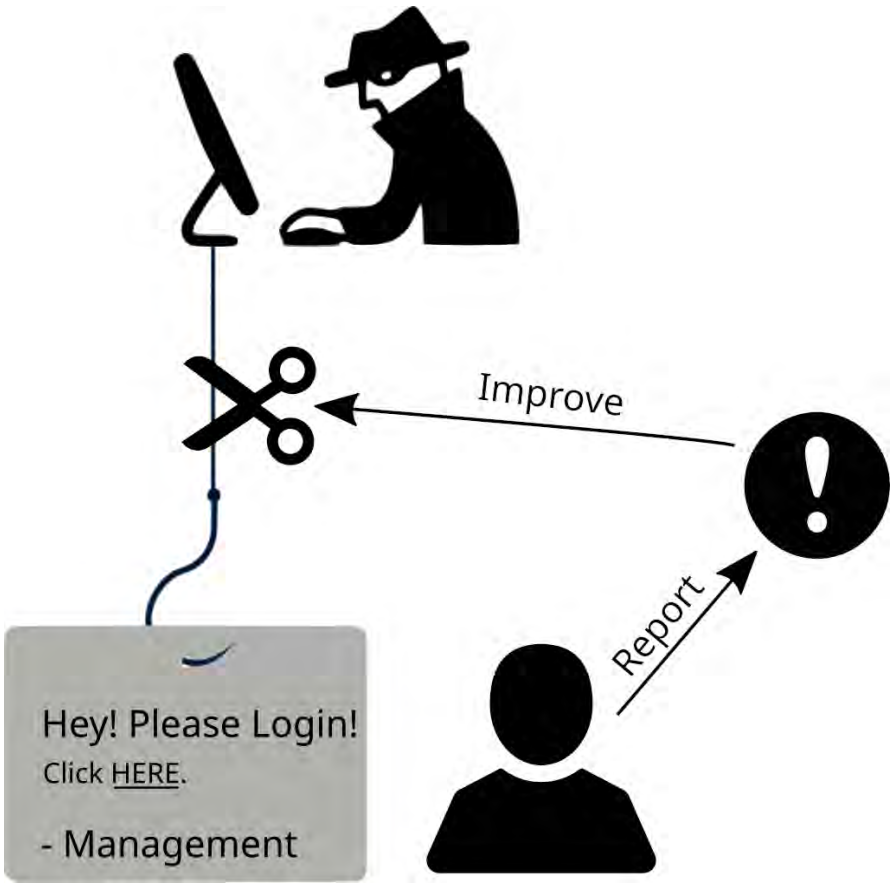
To further increase the resilience against attacks, in particular in the context of DDoS defense and IoT security, our architecture offers the option to hide paths from the public and thus to prevent attackers from flooding such invisible paths. Moreover, we have developed a scalable bandwidth-reservation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

Publications

C. Basescu, R. M. Reischuk, P. Szalachowski, A. Perrig, Y. Zhang, H. Hsiao, A. Kubota, J. Urakawa.
SIBRA: Scalable Internet Bandwidth Reservation Architecture
Symposium on Network and Distributed System Security (NDSS), 2016.

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.

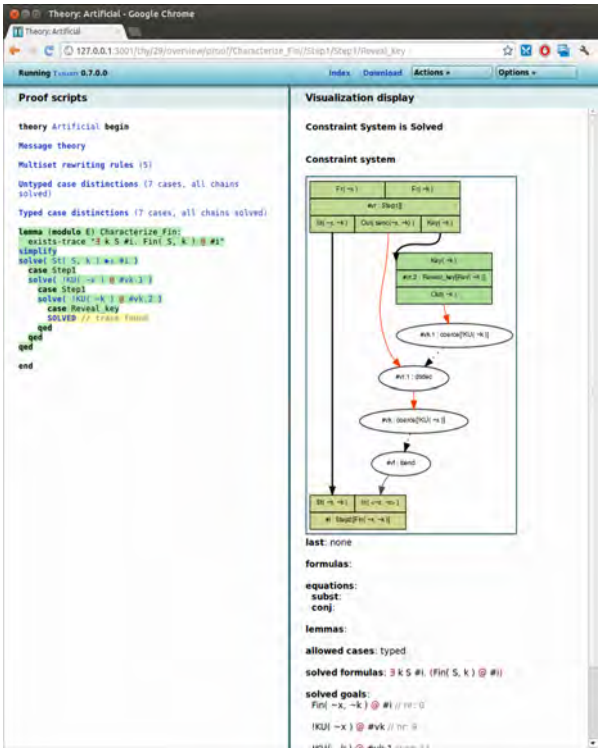
Moreover, we will analyze if user reports can be a useful first line of defense against 0-day phishing, by using reports to train machine learning classifiers that generate rules, instead of relying on burdensome manual creation by human experts.

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) that went into effect last year in Europe, 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.

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
IACR Cryptology ePrint Archive 2018

Industry partner
NEC

Towards Provably Secure Internet Communication

Internet applications rely heavily on secure communication. Problems such as lack of privacy, integrity or anonymity become a growing concern in the modern, globalized society. This is why the protocols designed to achieve such properties are of utmost importance.

Unfortunately, most of the currently used protocols, such as the TLS or the IPSec, often fail to provide clearly defined security guarantees. Indeed, every once in a while, a minor or even major vulnerability is discovered and then accordingly patched in the next version of a particular standard. One reason for this unsatisfactory situation is a somewhat ad-hoc design, without explicitly stated security goals and assumptions about the real world, and without security proofs. Known security analyses cover only partial aspects of the protocols.

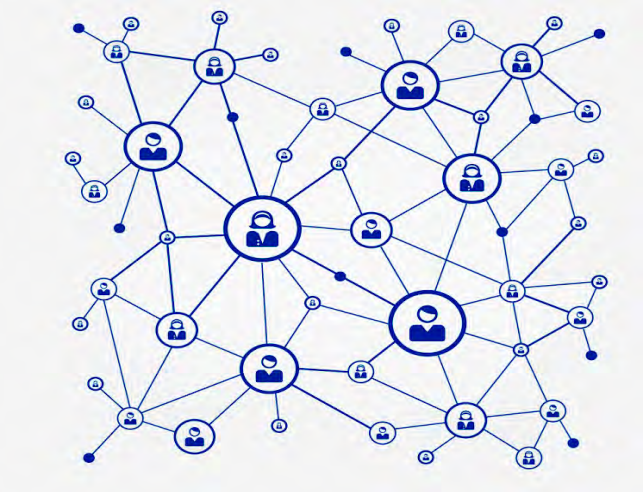
The goal of this project is to take a clean-slate approach to designing protocols for secure communication over the Internet. They will be designed in a systematic and modular fashion, with the goal of providing security underlying all of the design choices.

A thorough, formal security analysis will be conducted for all of the protocols, using the Constructive Cryptography framework. This will allow composable security statements about the different protocols to be formulated. Security of the composed protocols then follows from security of the individual components.

Some of the key issues we wish to address in the project include key agreement (where the key is authenticated either bilaterally or unilaterally), secure symmetric communication, forward secrecy (in the context of both pseudo-random generators and key agreement), leakage resilience and anonymity. We will also analyze security in the case where secret keys used are stolen, and aim to prove the consequences of such theft. More specifically, we study how does it affect the security of past encryptions and discuss what security statements one can still make in such a case.

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.

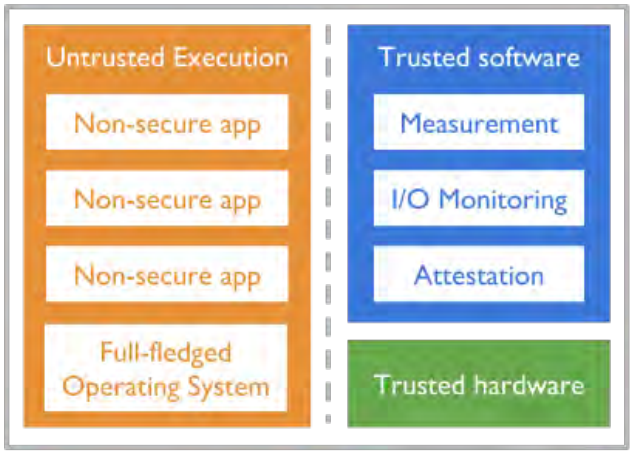
The goal of this project is to design topology-hiding communication protocols, which allow a set of parties connected by an incomplete network with unknown communication graph, where each party only knows its neighbors, to communicate in such a way that the network topology remains hidden even from a 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.

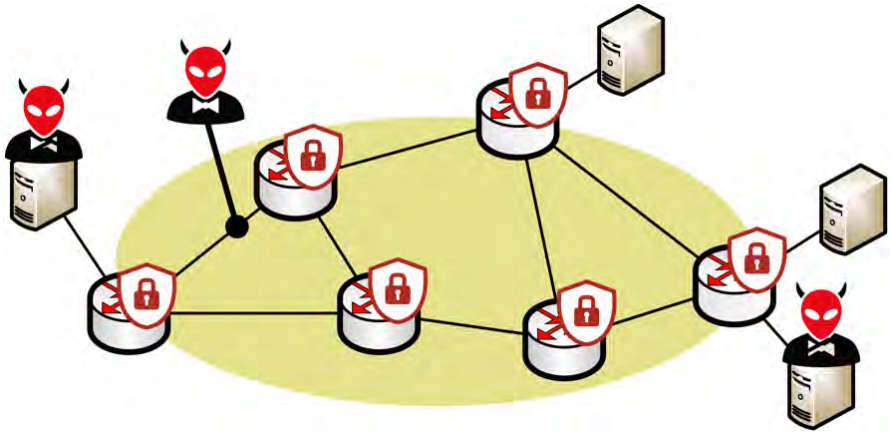
More recently, Arm has launched its Platform Security Architecture (PSA) framework, which aims to extend the security functionalities provided by the trusted environments. In this project we plan to investigate how these hardware components and architectures may be used to build powerful software tools 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

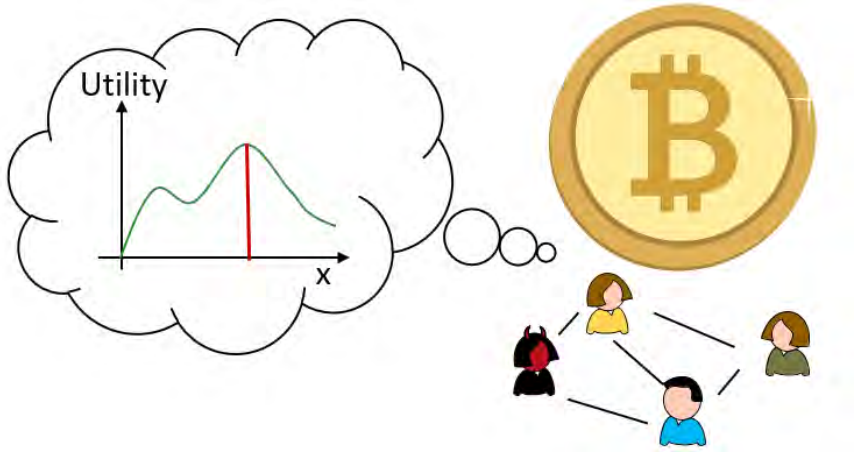
Roland Meier, David Gugelmann, Laurent Vanbever

iTAP: In-network Traffic Analysis Prevention using Software-Defined Networks

ACM SOSR 2017. Santa Clara, CA, USA (April 2017)Daniel Tschudi (Aarhus University)

For more details, see: https://itap.ethz.ch

Provably Secure Blockchains



This project aims to analyze the security of blockchain protocols from a provable security point of view. In a first phase, the goal is to formalize Bitcoin's ultimate goal as a ledger functionality in a universally composable language and to show that this functionality is securely realized by an appropriate abstraction of the Bitcoin protocol. The goal is to propose a ledger functionality that is general enough such that it can be realized also by other concrete blockchain protocols, hence becoming the standard security goal for blockchains in general. More specifically, we put forth a universally composable treatment of the Bitcoin protocol. We specify the goal that Bitcoin aims to achieve as a ledger functionality in the (G)UC model of Canetti et al. [TCC'07]. Our ledger functionality is weaker than the one recently proposed by Kiayias, Zhou, and Zikas [EUROCRYPT'16], but unlike the latter suggestion, which is arguably not implementable given the Bitcoin assumptions, we prove that the one proposed here is securely UC realized under standard assumptions by an appropriate abstraction of Bitcoin as a UC protocol.

In a second phase, the projects tries to challenge the assumptions behind the security proof. While the famous assumptions that the majority of the mining power is honest is widely accepted, the aim of this project is to investigate alternative assumptions such as rational assumptions on miners' incentives. In addition, the project tries to minimize assumptions, for example reducing the amount of synchrony that the protocols and the proofs rely on. We employ the machinery from the Rational Protocol Design (RPD) framework by Garay et al. [FOCS'13]. We show assuming a natural class of incentives for the miners' behavior (i.e., rewarding them for adding blocks to the blockchain but having them pay for mining), where one can reserve the honest majority assumption as a fallback, or even, depending on the application, completely replace it by the assumption that the miners aim to maximize their revenue. Our results underscore the appropriateness of RPD as a "rational cryptography" framework for analyzing Bitcoin. long the way, we devise significant extensions to the original RPD machinery that broaden its applicability to cryptocurrencies, which may be of independent interest.

Publications

C. Badertscher, U. Maurer, D. Tschudi, V. Zikas.
Bitcoin as a Transaction Ledger: A Composable Treatment.
Advances in Cryptology – CRYPTO 2017 – Proceedings, Part I, pp. 324-356, 2017.

C. Badertscher, J. Garay, U. Maurer, D. Tschudi, V. Zikas.
But Why Does it Work? A Rational Protocol Design Treatment of Bitcoin.
Advances in Cryptology – EUROCRYPT– Proceedings, Part II, pp. 34-65, 2018.

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

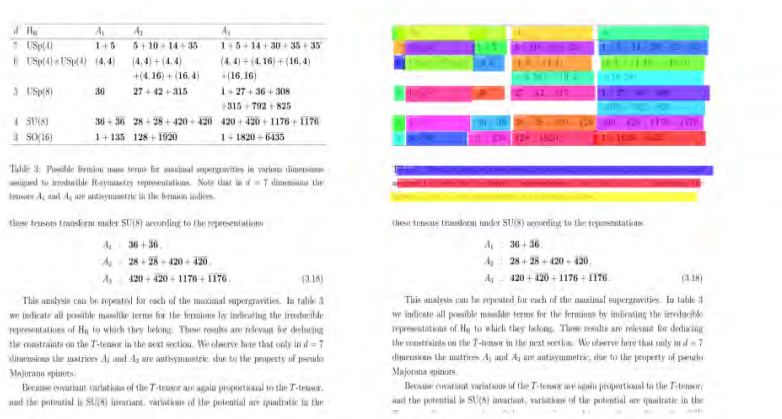
Christopher Portmann
Quantum Authentication with Key Recycling.
Advances in Cryptology – EUROCRYPT 2017 – Proceedings, Part III, pp. 339-368, 2017.

Research Projects

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.



Example of detection of tabular cells and captions (colored boxes) in an input document.

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 element detection, e.g. the prediction of the locations of 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. After this pretraining step, we can efficiently adapt our system to new document types without the need for manual adjustments of extraction heuristics.

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. 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