FRAUNHOFER INSTITUTE FOR SECURE INFORMATION TECHNOLOGY

CYBERSECURITY ANALYTICS AND DEFENCES
FORTIFY INTERNET SYSTEMS AND SERVICES
TRENDS
Modern societies continually face continuously emerging cyberspace threats. Most defences are not widely deployed, despite tremendous efforts to secure cyberspace, and existing countermeasures are often circumvented. In contrast, the extent and sophistication of attacks are on a constant rise. Attacks target critical infrastructures, cyber physical systems, financial organisations, email and web services, cloud platforms and data centres, users and the Internet infrastructure. The attacks deplete resources via denial of service, disrupt system functionality and operation and enable the perpetrators to intercept the communication, for example for surveillance, censorship, malware distribution or credentials theft.

Fraunhofer SIT is focused on fortifying the foundations of the Internet, and on developing easy to deploy defences, to ensure Internet security and availability. To that end, we study the vulnerabilities in the standards and the design of the systems and services deployed in the Internet, we research challenges and obstacles towards adopting cryptographic schemes for system and network defences and study faulty cryptography deployments.

RESEARCH
Our research topics cover the following areas:

- **Defences against Denial of Service (DoS) attacks:**
  We design and develop easy to deploy and effective defences preventing DoS attacks.

- **Detection of malware and Advanced Persistent Threats (APTs):**
  A large section of the Internet computers is infected with malware (malicious software). Attackers can exfiltrate sensitive user data (such as credentials, passwords or credit card numbers), eavesdrop on communication, or exploit compromised computers in DoS campaigns. We develop network based malware detection techniques.

- **Design and adoption of cryptographic schemes:**
  Integrating cryptography into Internet systems entails multiple challenges and obstacles. We use Internet measures for inferring the topology and configuration of Internet networks and services, and adjust the cryptographic schemes to match and interoperate with the existing systems.

- **Privacy and anonymity:**
  Data and communication privacy is essential for the economy, Internet autonomy and safety. We design privacy preserving communication protocols, to ensure efficiency and quality of service.
SERVICES

Fraunhofer SIT provides access to the results of applied science and its experience in the respective industries. In Cybersecurity Analytics and Defenses our services focus on:

- **Internet infrastructure**: Security of the fundamental building blocks such as routing and naming systems that comprise the foundations of the Internet is critical to the security and stability of Internet clients and services. Unfortunately, the Internet infrastructure and the services it provides are subject to numerous attacks. We research vulnerabilities in the Internet infrastructure such as those that allow intercepting communication, and design countermeasures to prevent attacks.

- **Industrie 4.0 and cyber physical systems**: Elements involved in the production of Industrie 4.0 are interconnected among themselves and the Internet. Cyberphysical systems monitor physical processes, sensors and devices. Within this context we also study industrial control systems, SCADA in particular. Securing communication is substantial to preventing catastrophic events and incidents. We research fault tolerance and evaluate vulnerabilities pertaining to communication between the devices on the grid.

- **Cloud platforms**: Cloud offers a convenient platform to provide hosting and service management to customers. However, coresidence and platform sharing between multiple customers (often with conflicting interests) introduces new security challenges. We research security aspects, such as isolation on a network layer and infrastructure guarantees provided by the cloud platform.

- **Web**: A majority of the attacks against end users exploit vulnerabilities in the web and in vulnerable or incorrectly deployed cryptographic mechanisms. Securing the web is critical to enabling clients to perform online transactions and communications, and important for guaranteeing service providers’ profits. We evaluate the security of browsers, and communication channels.

- **Voice over IP and mobile communication**: Telephony is operated increasingly over IP networks. Intercepting phone communication is detrimental to the privacy and security of individuals, organisations and governments. We investigate vulnerabilities that may be exploited by attackers and design countermeasures to prevent them.
THE INSTITUTE

The Fraunhofer Institute for Secure Information Technology SIT is one of the oldest and most respected research institutes for IT security in the world. More than 160 employees support companies and government bodies in securing data, services, infrastructures, and end products. Fraunhofer SIT is part of a multi-faceted research landscape with a focus on IT security.

In Darmstadt more than 300 researchers are working on IT security related topics. The Institute and its employees are active members of the European Center for Security and Privacy by Design (EC SPRIDE), which is supported by the Ministry of Education and Research, and the Center for Advanced Security Research Darmstadt (CASED), which is supported by the state of Hesse.

CONTACT

Prof. Dr. Michael Waidner
Phone: +49 6151 869-282
Fax: +49 6151 869-224
michael.waidner@sit.fraunhofer.de

Fraunhofer Institute for Secure Information Technology
Rheinstrasse 75
64295 Darmstadt
www.sit.fraunhofer.de

Dr. Haya Shulman
Phone: +49 6151 869-505
Fax: +49 6151 869-224
haya.shulman@sit.fraunhofer.de

Fraunhofer Institute for Secure Information Technology
Rheinstrasse 75
64295 Darmstadt
www.sit.fraunhofer.de