Here is a brief outline of the topics covered by Mr. Reinhard during his GuestLecture on Internet Security! *Note links available below as well!*

Topics in Security

IBM Security / Threat Intelligence Portal
http://exchange.xforce.ibmcloud.com

IBM Security http://www.ibm.com/security/
- Security intelligence and analytics
- Identity and access management
- Application security
- Advanced fraud protection
- Data security and privacy
- Infrastructure protection

IBM X-Force
http://www-03.ibm.com/security/xforce/
X-Force Research in numbers:
32B Analyzed web pages and images
100K Documented vulnerabilities
8M Spam and phishing attacks daily
20B Events managed per day
860K Malicious IP addresses
270M Endpoints monitored for malware

IBM X-Force Research: Security Trends in the Energy and Utilities Industry
https://securityintelligence.com/media/xforce-research-security-trends-in-the-energy-and-utilities-industry/

Krebs on Security
https://krebsonsecurity.com/

CVE Common Vulnerabilities and Exposures
https://cve.mitre.org/

SCADA
SCADA (supervisory control and data acquisition) is a category of software application program for process control, the gathering of data in real time from remote locations in order to control equipment and conditions. SCADA is used in power plants as well as in oil and gas refining, telecommunications, transportation, and water and waste control.

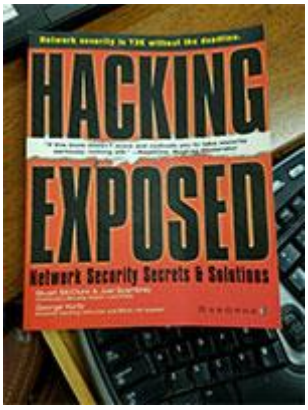
SCADA systems include hardware and software components. The hardware gathers and feeds data into a computer that has SCADA software installed. The computer then processes this data and presents it in a timely manner. SCADA also records and logs all events into a file stored on a hard disk or sends them to a printer. SCADA applications warn when conditions become hazardous by sounding alarms.

IoT
2016-11-09 ZigBee
IoT Goes Nuclear: Creating a ZigBee Chain Reaction
http://iotworm.eyalro.net/iotworm.pdf

DDoS
2016-06-20 -> Akamai Report: 363 Gbps DDoS Attack
2016-11-07 DDoS
DDoS attack halts heating in Finland amidst winter
A Distributed Denial of Service (DDoS) attack halted heating distribution at least in two properties in the city of Lappeenranta, located in eastern Finland.
In both events the attacks disabled computers that were controlling heating in the buildings.
4G Cellular Networks At Risk Of DoS Attacks
Black Hat Europe researcher shows how hackers can conduct denial-of-service attacks on 4G cellular devices around the world.

Passwords
Length is the most important criterium for a secure password, i.e. more than 12 characters, aside, of course, from not being found in a dictionary.
Unfortunately, many sites limit password length to less than that, which requires some other complexity rules to achieve a certain level of security.

2FA
What is two-factor authentication?
Two-factor authentication adds a second level of authentication to an account log-in. When you have to enter only your username and one password, that's considered a single-factor authentication. 2FA requires the user to have two out of three types of credentials before being able to access an account. The three types are:
- Something you know, such as a personal identification number (PIN), password or a pattern
- Something you have, such as an ATM card, phone, or fob
- Something you are, such as a biometric like a fingerprint or voice print



White Hat / Ethical Hacker
Job Description: What Does an Ethical Hacker Do?
Ethical hackers evaluate computer systems and networks by trying to break them,e.g. by performing penetration testing and reverse engineering. They probe assets' security by trying

to compromise hardware or software by using known vulnerabilities or designing new entry vectors on-the-fly. They do not like to be confused with script kiddies.

Pen(etration) Tester
Job Description
A penetration tester is a special type of network security consultant (White Hat or Ethical Hacker) who attempts to break into computer systems. They typically run a variety of tests, generally based on network penetration tools like Metasploit, resulting in security assessment reports. They may run those tests out-of-the-box but likely design their own custom tests, which requires creativity and patience along with the in-depth knowledge of programming languages and software applications.

Defensive Programming / Secure Programming / buffer overflow / input validation / canonicalization
SEI CERT Secure Coding Standards
https://www.securecoding.cert.org/confluence/display/seccode/SEI+CERT+Coding+Standards

SEI CERT Oracle Coding Standard for Java
https://www.securecoding.cert.org/confluence/display/java/SEI+CERT+Oracle+Coding+Standard+for+Java

Secure Programming HOWTO - Creating Secure Software
http://www.dwheeler.com/secure-programs/

Zero-Day Exploits
Zero-Day Exploits take advantage of a security vulnerability on the same day that the vulnerability becomes publicly or generally known, i.e. without enough time for the vendor to react.

Phishing
FBI: $2.3 Billion Lost to CEO Email Scams
https://krebsonsecurity.com/2016/04/fbi-2-3-billion-lost-to-ceo-email-scams/

Social Engineering
One name says it all: Kevin Mitnick.
"Social engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he isn't, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology."
His books are The Art of Deception; The Art of Intrusion; Ghost in the Wires: My Adventures as the World's Most Wanted Hacker.
Yes, he was 5 years in prison for various crimes.

and in other news ...:

2016 Bangladesh Bank heist
https://en.wikipedia.org/wiki/2016_Bangladesh_Bank_heist
In February 2016, instructions to steal US$951 million from Bangladesh Bank, the central bank of Bangladesh, were issued via the SWIFT network. Five transactions issued by hackers, worth $101 million and withdrawn from a Bangladesh Bank account at the Federal Reserve Bank of New York, succeeded, with $20 million traced to Sri Lanka (since recovered) and $81 million to the Philippines (about $18 million recovered).[1] The Federal Reserve Bank of NY blocked the remaining thirty transactions, amounting to $850 million, at the request of Bangladesh Bank.[2]

That Insane, $81M Bangladesh Bank Heist? Here's What We Know
https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/

On February 4, unknown hackers used SWIFT credentials of Bangladesh Central Bank employees to send more than three dozen fraudulent money transfer requests to the Federal Reserve Bank of New York asking the bank to transfer millions of the Bangladesh Bank's funds to bank accounts in the Philippines, Sri Lanka and other parts of Asia.

The hackers managed to get $81 million sent to Rizal Commercial Banking Corporation in the Philippines via four different transfer requests and an additional $20 million sent to Pan Asia Banking in a single request (which was reversed). But the Bangladesh Bank managed to halt $850 million in other transactions. The $81 million was deposited into four accounts at a Rizal branch in Manila on Feb. 4, 2016.

The hackers might have stolen much more if not for a typo in one of the money transfer requests that caught the eye of the Federal Reserve Bank in New York. The hackers apparently had indicated that at least one of the transfers should go to the Shalika Foundation, but they misspelled "foundation" as "fandation."