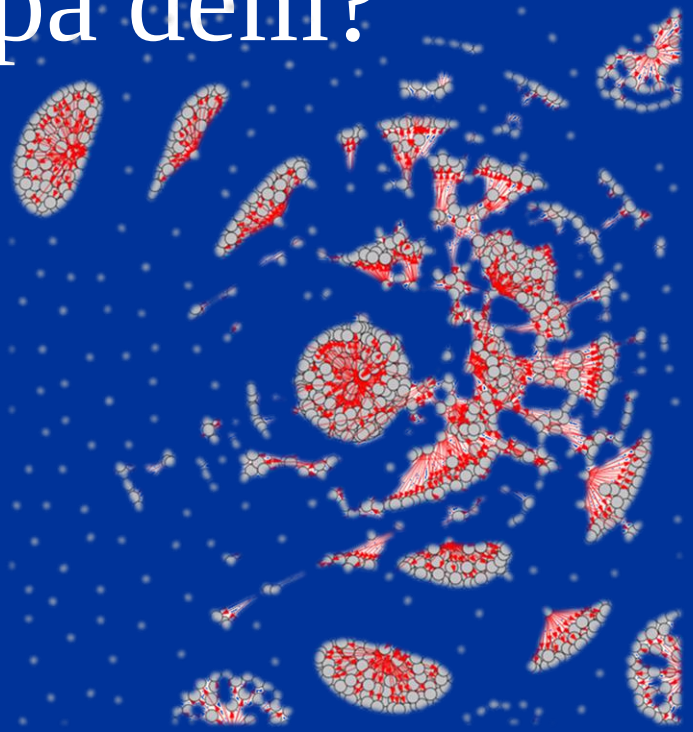
Datorer finns överallt, men kan man lita på dem?

Magnus Almgren

Göteborg 2017-10-19



Security Quiz

- Connect to kahoot.it
  - Enter Pin: xxxx (will come when I start the quiz)
- FAQ
  - Questions appear on full screen
  - You press the answer (based on color, symbol) on your device
  - The faster you press the correct answer, the more points
  - Sometimes, several answers may be correct

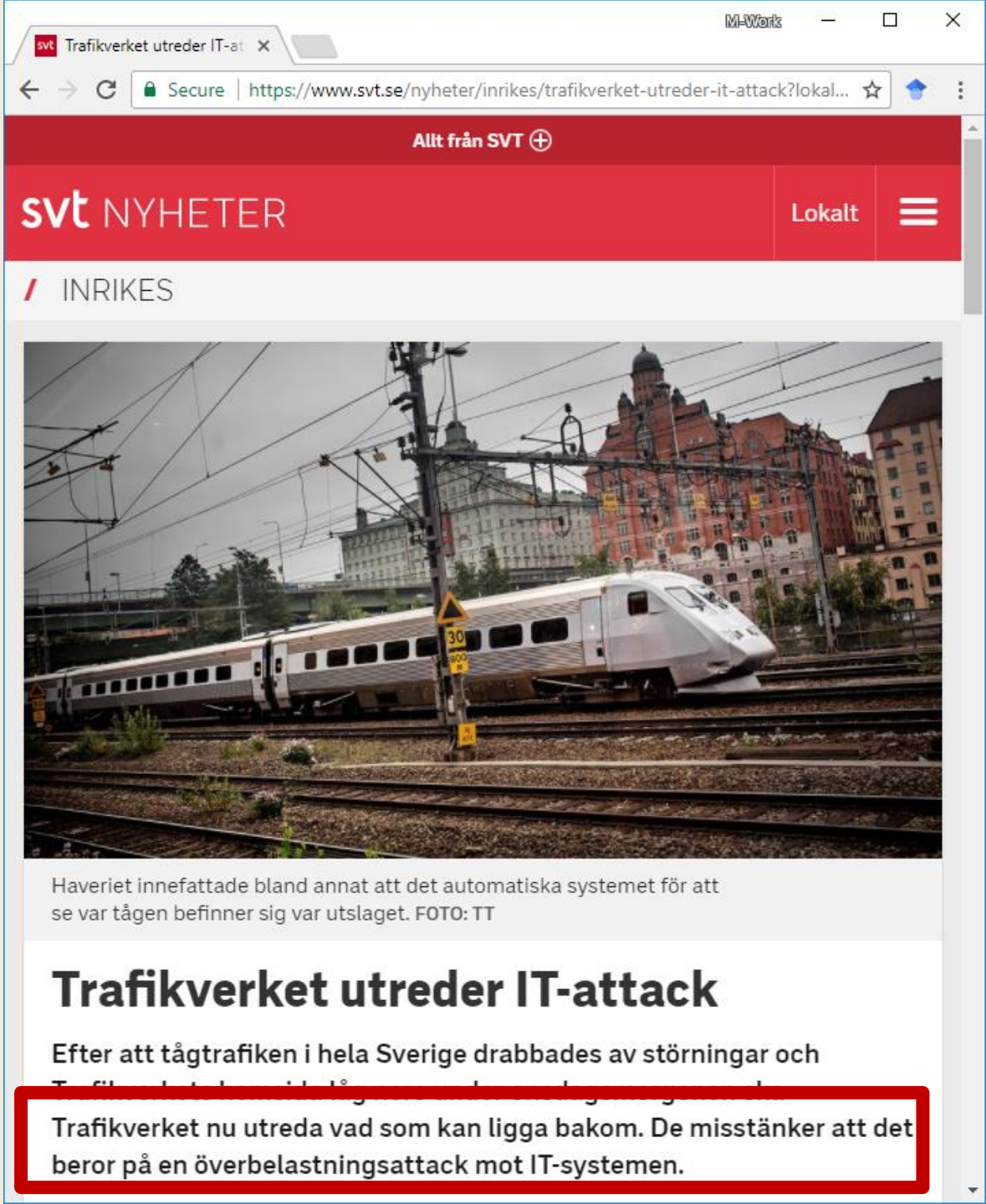
- Good luck!

15—20 år sedan …

- Internet började att användas av fler, men
  - de flesta hade inte ens e-post, och
  - datasäkerhet var något man ofta inte tänkte på.
- Den typiska hackern beskrevs ofta som en
  - tonåring,
  - som såg attacken som“schackspel”
  - **mål:** inbördes beundran inom en liten krets …
- Och idag ?

Dagliga attacker …

- De misstänker att det beror på en över-belastnings-attack mot IT-systemen.



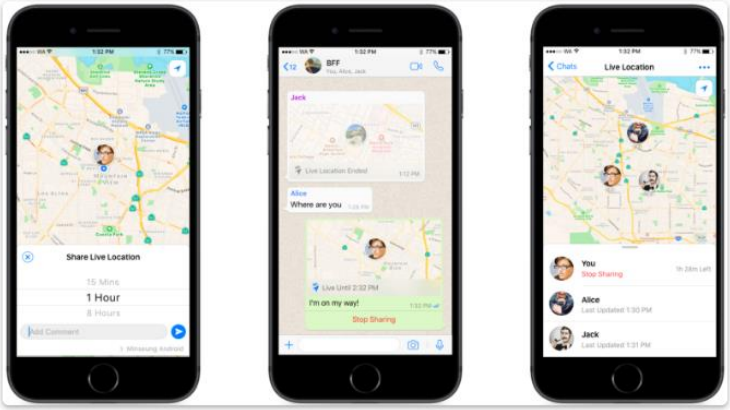
Dagliga attacker …

- De misstänker att det beror på en över-belastnings-attack mot IT-systemen.


20:50
Rocio
last seen today at 11:53
träffas på Skandinavium 22:21
På lördags jag skulle gärna gå hoss dig! 22:21
Vi kan träffas hos mig fredag runt 1730 22:23
Ok! Vi kan gå där. Jag kan laga något, empanada eller tortilla 22:51
Och ta den till dig 22:51
22:51
Det låter bra. Vi återkommer fredag med mer detaljer 23:30
APRIL 6, 2016
Messages you send to this chat and calls are now secured with end-to-end encryption. Tap for more info.
Type a message

WhatsApp får krypterad platsdelning

7 Swedroid / by Lars A / 12 hours ago



Senaste finessen i meddelandetjänsten WhatsApp är platsdelning i realtid. Delningen är krypterad (E2EE) precis som all övrig kommunikation i appen.

Användare väljer vilka kontakter de vill

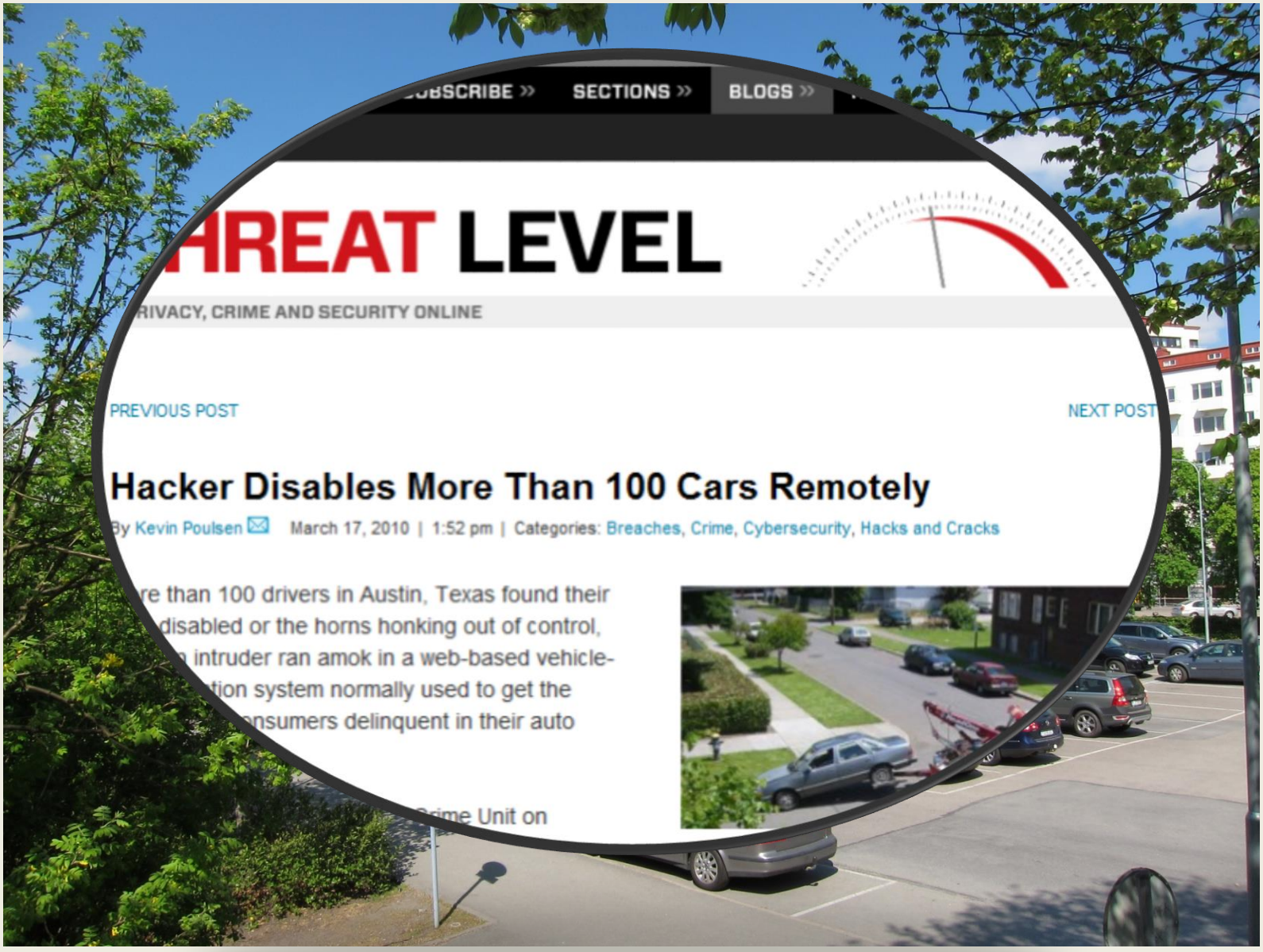
Översikt

- Bakgrund
  - Vad attackeras? Vilka gör det?
- Vad är en datorattack?
- Vad ska man tänka på?
- Vad sker inom forskningen?
- Hur kan jag lära mig mer?
  - Kurser?
  - Grupper på Chalmers/GU?

Var finns ”datorer” i samhället

- ”vanlig” dator
- surfplatta, mobiltelefon
- TV-spel, musikspelare, …


Hack-ad
dator


SUBSCRIBE »
SECTIONS »
BLOGS »
HREAT LEVEL
RIVACY, CRIME AND SECURITY ONLINE
PREVIOUS POST
NEXT POST
Hacker Disables More Than 100 Cars Remotely
By Kevin Poulsen
March 17, 2010 | 1:52 pm | Categories: Breaches, Crime, Cybersecurity, Hacks and Cracks
re than 100 drivers in Austin, Texas found their
disabled or the horns honking out of control,
intruder ran amok in a web-based vehicle-
tion system normally used to get the
nsumers delinquent in their auto
rime Unit on


Morning Herald
MEGA SHOW
PART 1
20-23 Octo
Technology
News
Biz-Tech
Security
Enterprise
Sci-Tech
Blogs
Digital Life
Compare & Save
You are here: Home » Technology » Security » Article
'Sinister' Integral Energy virus outbreak a threat to power grid
Asher Moses
October 1, 2009

And even lamps need security

First version used a hash of the MAC address of the device to handle the authentication …

http://www.meethue.com/en-US

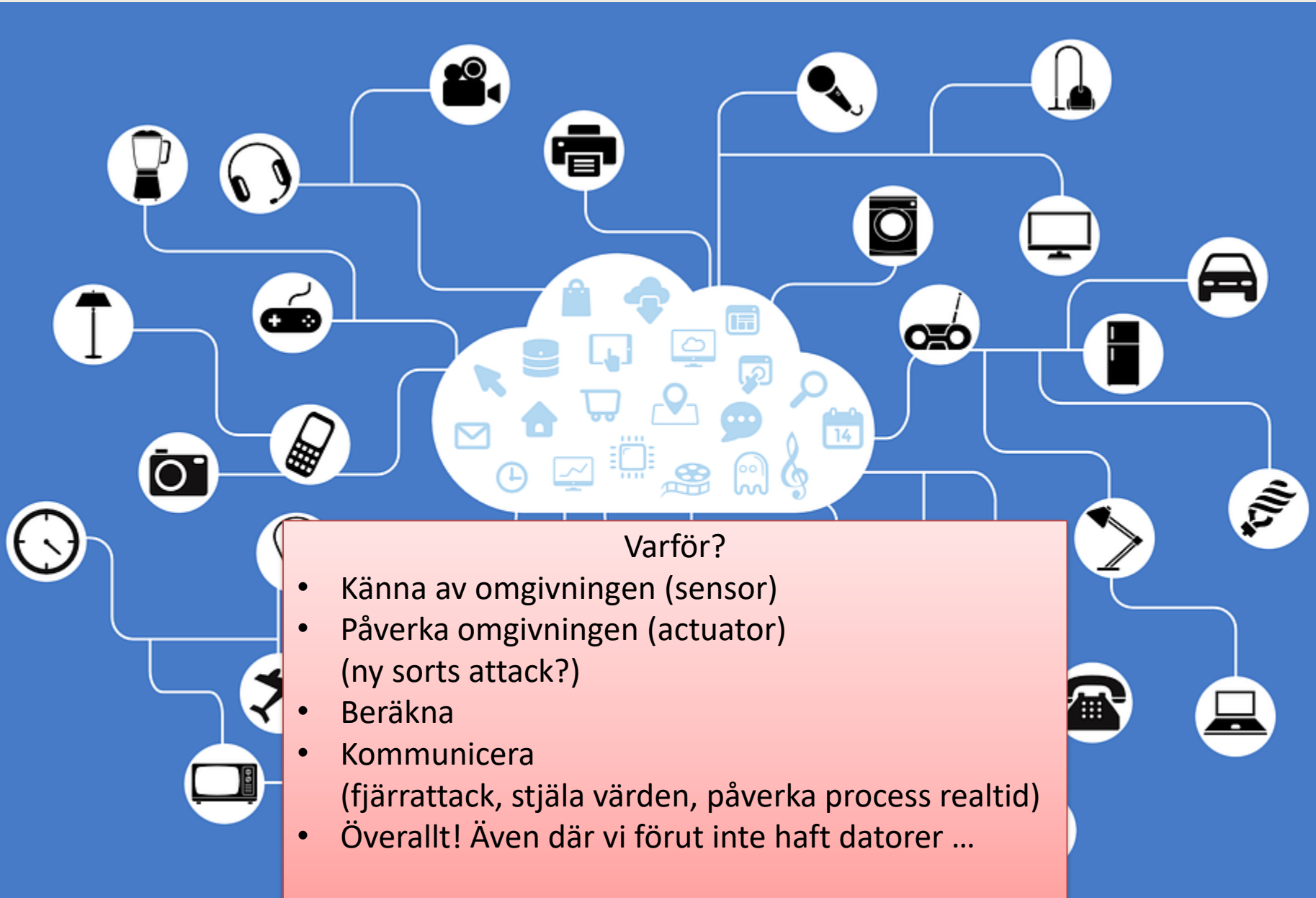
https://commons.wikimedia.org/wiki/File:St_Jude_Medical_pacemaker_in_hand.jpg

Var finns ”datorer” i samhället

- ”vanlig” dator
- surfplatta, mobiltelefon
- tvspelskonsol, musikspelare, …
- kopieringsmaskin, annan kontorsutrustning
- bil, flygplan, tåg (och system runt omkring)
- samhällskritiska system: bankväsende, elförsörjning, transporter
- medicintekniska produkter: pacemaker …

Internet of Things

Internet of Things

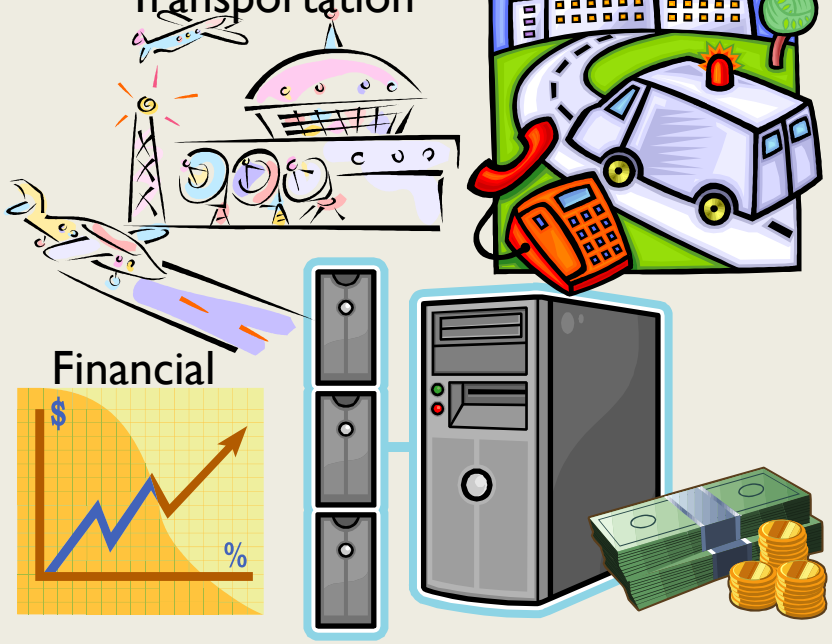


Varför?

- Känna av omgivningen (sensor)
- Påverka omgivningen (actuator)
  (ny sorts attack?)
- Beräkna
- Kommunicera
  (fjärrattack, stjäla värden, påverka process realtid)
- Överallt! Även där vi förut inte haft datorer …

Health care

Transportation



Financial

Snowden framträder i Göteborg

Edward Snowden. Foto: TT

I dag framträder mannen som läckte topphemlig information om USA:s massövervakning mot vanliga medborgare i Göteborg. Edward Snowden medverkar vid en konferens för grävande journalister i Göteborg, Gräv 2016.

Och det är en stolt Nils Hanson, chef för SVT:s Uppdrag Granskning och "Grävgeneral", som försöker värdera hans medverkan.


Xi Jinping's Marathon Speech: Five Takeaways


Samsung Is Under Scrutiny Again as South Korean Police Raid Offices


U.S. Stood by as Indonesia Killed a Half-Million People, Papers Show


Rohingya Refugees Fleeing Myanmar Await Entrance to Squalid Camps

The World Once Laughed at North Korean Cyberpower. No More.

繁體中文版 | 繁體簡體中文版

By DAVID E. SANGER, DAVID D. KIRKPATRICK and NICOLE PERLROTH OCT. 15, 2017

A military officer who teaches computer science at the Mangyongdae Revolutionary School, on the outskirts of Pyongyang, North Korea. Alexander F. Yuan/Associated Press

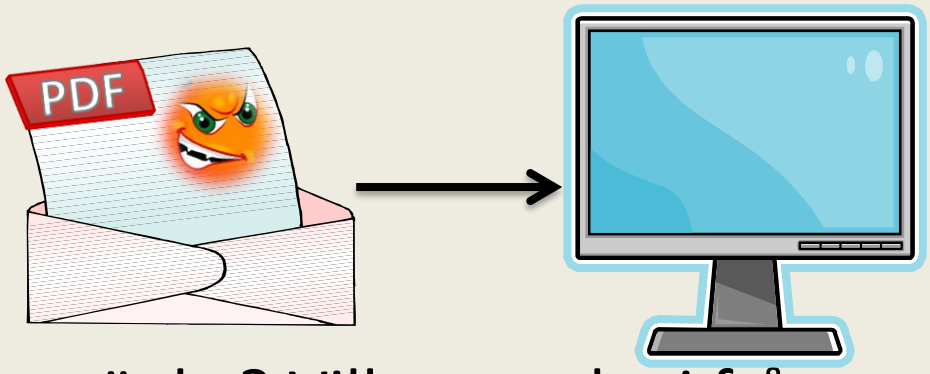
When North Korean hackers tried to steal $1 billion from the New York Federal Reserve last year, only a spelling error stopped them. They were digitally looting an account of the Bangladesh Central Bank, when bankers grew suspicious about a withdrawal request that had misspelled "foundation" as "fandation."

RELATED COVERAGE

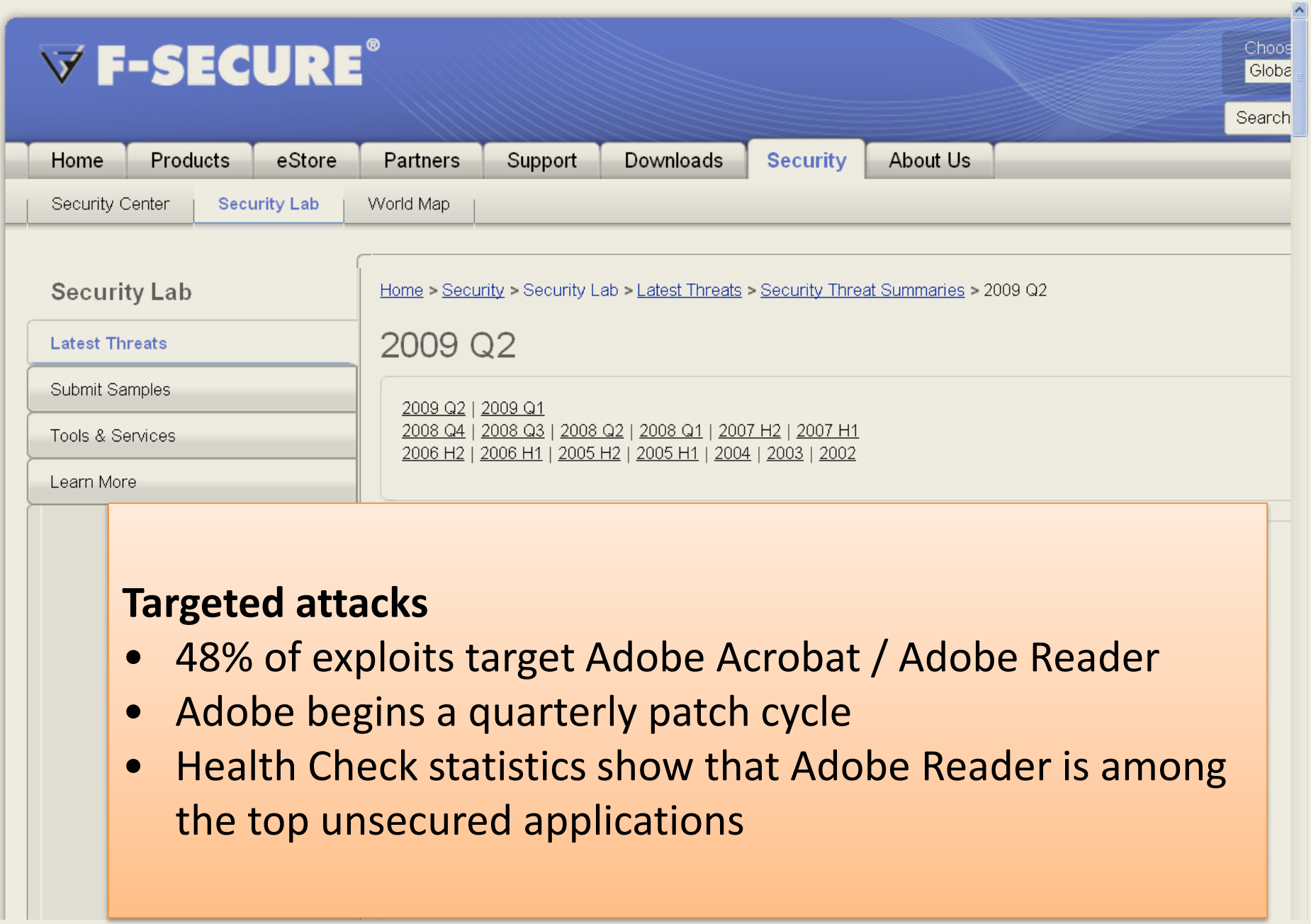

U.S. Weighs Response to Sony Cyberattack, With North Korea Confrontation Possible

Skadlig kod

- **Många användare säger:**
  Jag laddar aldrig ner filer med osäkert innehåll!
- Men när är man egentligen säker?
  - Ladda ned körbar kod?
  - Titta på ett PDF-dokument?



- Hur ska man tänka? Vilken analogi från verkliga livet fungerar?



Targeted attacks

- 48% of exploits target Adobe Acrobat / Adobe Reader
- Adobe begins a quarterly patch cycle
- Health Check statistics show that Adobe Reader is among the top unsecured applications

http://home.mcafee.com/AdviceCenter/most-dangerous-celebrities

Dangerous People (!!!)

Cameron Diaz Searches Yield Ten Percent Chance of Landing on a Malicious Site

Treasure

Förklaring av datorattacker

- En hacker följer inte instruktioner!
- Hon försöker bryta programmet och finna svagheter.

Inloggning

Lösenord: __ __ __ __ __ __

(max 6 tecken, tre försök)

Förklaring av datorattacker

- En hacker följer inte instruktioner!
- Hon försöker bryta programmet och finna svagheter.
- **Lura människor (”social engineering”)**

Förklaring av datorattacker

- En hacker följer inte instruktioner!
- Hon försöker bryta programmet och finna svagheter.
- Lura människor (”social engineering”)
- **Och flera andra sätt med tekniska namn**
  - **TOCTOU-attack = kontrollen sker inte när filen används**
  - **Korrumpera minnet (buffer overflow)**
  - **Etc.**

Denial-of-service attack

- Attackerar **tillgängligheten** till systemet:
  - Bandbredd
  - CPU
  - Andra resurser
- Alla system sårbara i viss mån
- Angriparen skapar först ett ”botnet” genom att smitta vanliga användare
- Därefter attackerar alla smittade datorer samma mål

Security is the lack of insecurity!

Att tänka på som användare

- Säkerhet är alltid en balansgång
- Vad vill man skydda? Till vilket pris?
- Några konkreta råd
  - Uppdatera systemet
  - Uppdatera alla program
  - Använd antivirus
  - Använd en brandvägg
  - Fundera på lösenorden
- Krypterad kommunikation viktig, mer behövs(!)

Forskning
Industriella Kontrollsystem

- Körs i realtid
  - Respons tidskritisk
- Tillgänglighet 7x24
  - Omstarter kan vara oacceptabla
- Säkerhet = ”safety” är viktigt!
- Gamla (”legacy system”) med nya system
  - Öppna standarder men även skräddarsydda protokoll.
- Lång livslängd

Annan forskning

- Algoritmer för smarta elnät
- Säkrare bilar
- Men även bättre stöd för att bygga komplicerade system.
  - Detektering av ”botnets”
  - Privacy (personlig integritet) etc.
  - Bättre filtrering av skräppost

Doktorera? Kontakta oss tidigt och arbeta med oss!

Exjobb? Öka chanser för industrin?

http://www.cse.chalmers.se/edu/master/secspec/

Where to go from here?

protection. Modeling and assessment of security and dependability as well as metrication methods are covered. A holistic security approach is presented and organizational, business-related, social, human, legal and ethical aspects are treated.

Runs in study period 3

broken protocols are also discussed to enhance understanding of the engineering difficulties in building secure systems.

Runs in study period 2

perspective of attack vs. protection is threaded through the lectures, laboratory assignments, and projects.

Runs in study period 4.

security protocols such as SSL, SSH and IPsec. Knowledge about possible threats and countermeasures is important for understanding what level of security a system and an application can offer.

Runs in study period 4

Security is becoming increasingly important for system design and development. System architects and designers must have security expertise, so that the systems they design do not fall victims to attacks. Software developers and engineers must have security expertise, so that the code they produce cannot be exploited. Security and network specialists must have critical knowledge of security principles and practice, in order to ensure the security of the systems they are responsible for.

Strong ties with industry

OWASP We have tight relations with the Open Web Application Security Project (OWASP). We are actively involved in both the Stockholm and Gothenburg OWASP chapters.

Cutting edge research

Crisalis is an EU project on security analysis for critical infrastructures in collaboration with eight academic and industrial partners across Europe.

CRISALIS
SECURING CRITICAL INFRASTRUCTURES

Goals

- Letting students from computer science and other disciplines be introduced to advanced interdisciplinary concepts related to the smart grid, thus
- building an understanding of the vocabulary and important terms that may have different meanings in the individual disciplines, and
- investigating a domain-specific problem relevant to the smart grid that need an understanding beyond the traditional ICT field.

DAT300/DIT668
DATA-DRIVEN SUPPORT FOR CYBER-PHYSICAL SYSTEMS

Goals

Letting students from computer science and other disciplines be introduced to advanced interdisciplinary concepts related to the smart grid, thus

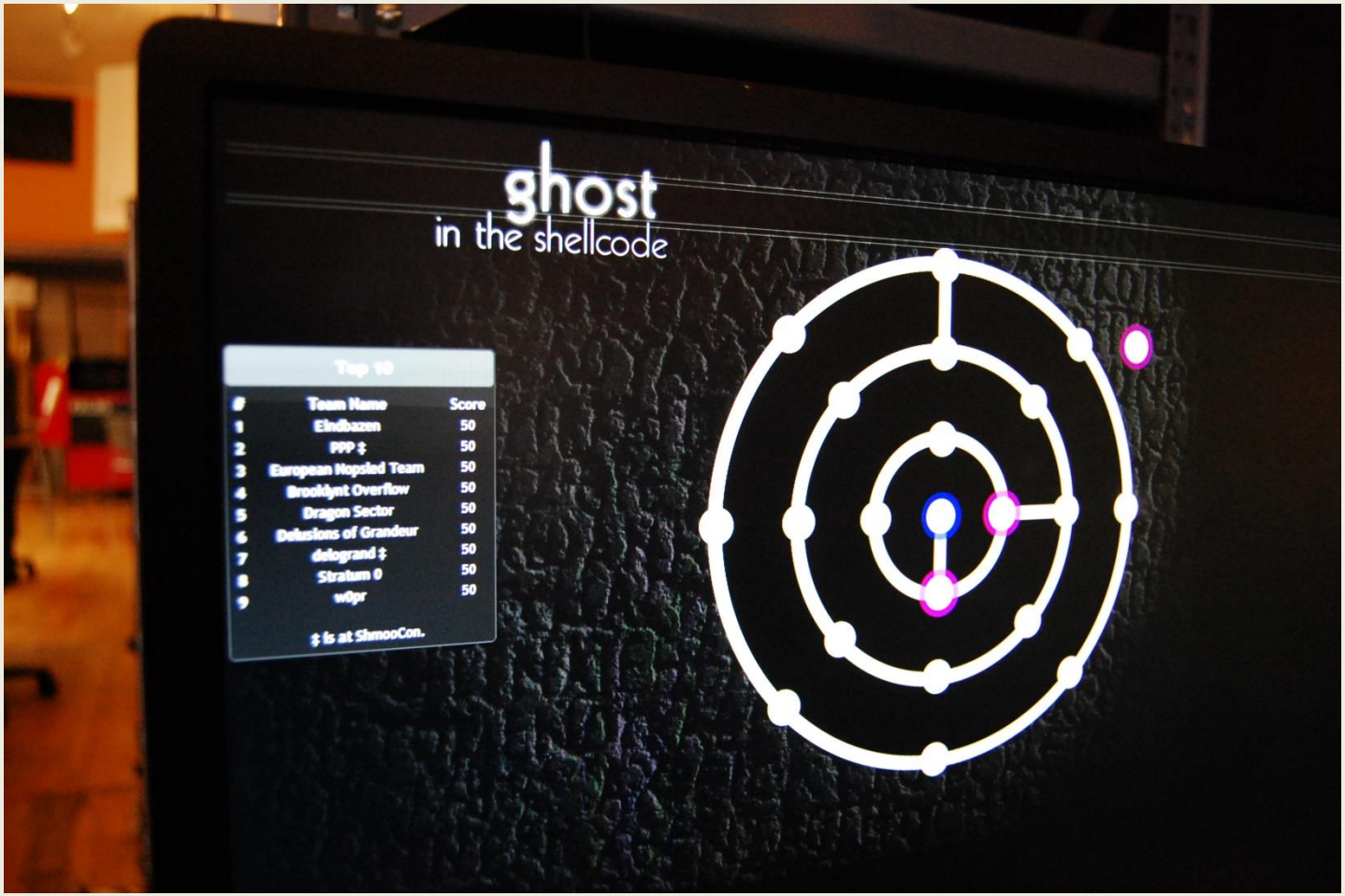
building an understanding of the vocabulary and important terms that may have different meanings in the individual disciplines, and

investigating a domain-specific problem relevant to the smart grid that need an understanding beyond the traditional ICT field.

- YES! I would want more courses like this course. I feel like I've learned so much more than I do in traditional courses.

  I also like the close connection to research since, it is often missing in traditional courses.
- I have never spent so much time on a course.

Competition
Capture the Flag



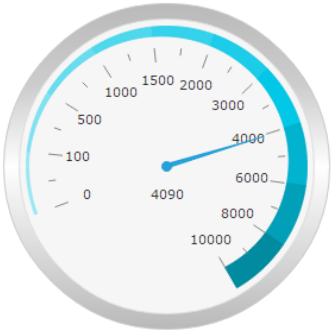
https://www.facebook.com/chalmersctf/

10K STUDENTS TO IMPROVE CYBER SECURITY

An Initiative of the SysSec Consortium

What is the 10KStudents Challenge?

The goal of the 10KStudents challenge is to improve cyber security by teaching **Ten Thousand University Students** the basic concepts of software vulnerabilities and secure programming. The challenge will teach students that security is inherent to all steps of building an IT system – not a property that can be added in the last step of the development cycle.



We reach out to all faculty members teaching programming and/or system design courses to participate in our challenge to increase cyber security. The challenge consists of three parts/lectures of increasing difficulty, all centered around the notorious **buffer overflow** bug:

- **General Introduction**
- Part I - **Basic Buffer Overflows** (Everyone)
- Part II - **Real Buffer Overflows** (Computer Scientists)
- Part III - **Countermeasures** (Students in Security courses)

If you would like to be part of the challenge that will educate more than ten thousand students in cyber security join us **here**.

"…because several is not a number and later is not a time
*The time is **now** and the number is **10,000**…"*

Finally…..

It is obvious that there are a large number problems to be addressed…..

……and the Computer Security courses won't solve them!

(but hopefully it will provide a deeper understanding!)