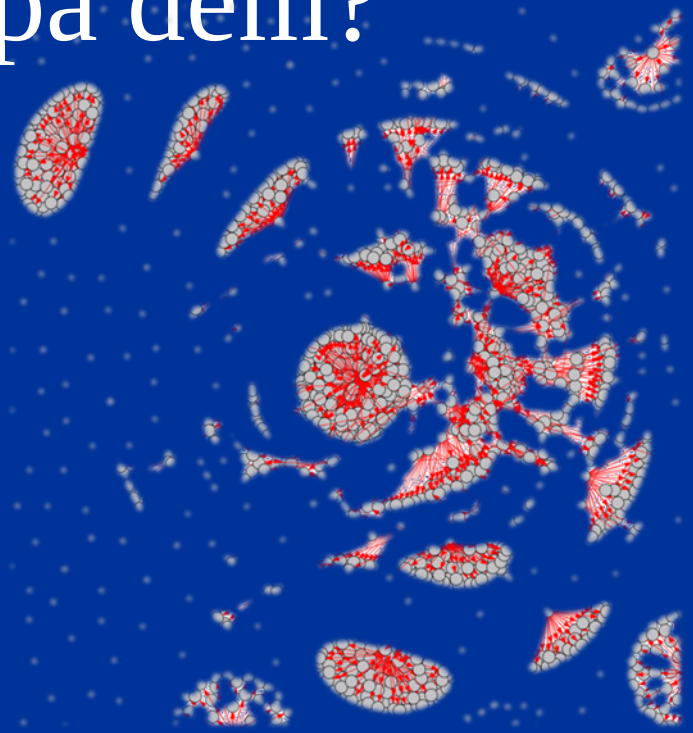
Datorer finns överallt, men kan man lita på dem?

Magnus Almgren

Göteborg 2015-05-20

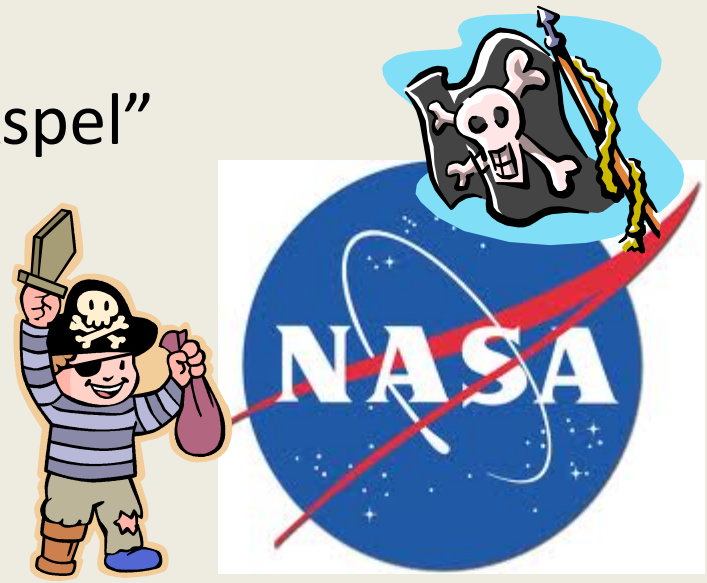


Security Quiz

- 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 ?



SVT Documentary oct-10, 2010: Att hacka en stormakt (http://goo.gl/1Zrd)

Översikt

- Bakgrund
  - Vad attackeras? Vilka gör det?
- Vad är en datorattack?
- Vad ska man tänka på?
- Vad sker inom forskningen?
- Vilka kurser finns för att lära sig mer?

Var finns ”datorer” i samhället

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


Hacksåg
dator

Var finns ”datorer” i samhället

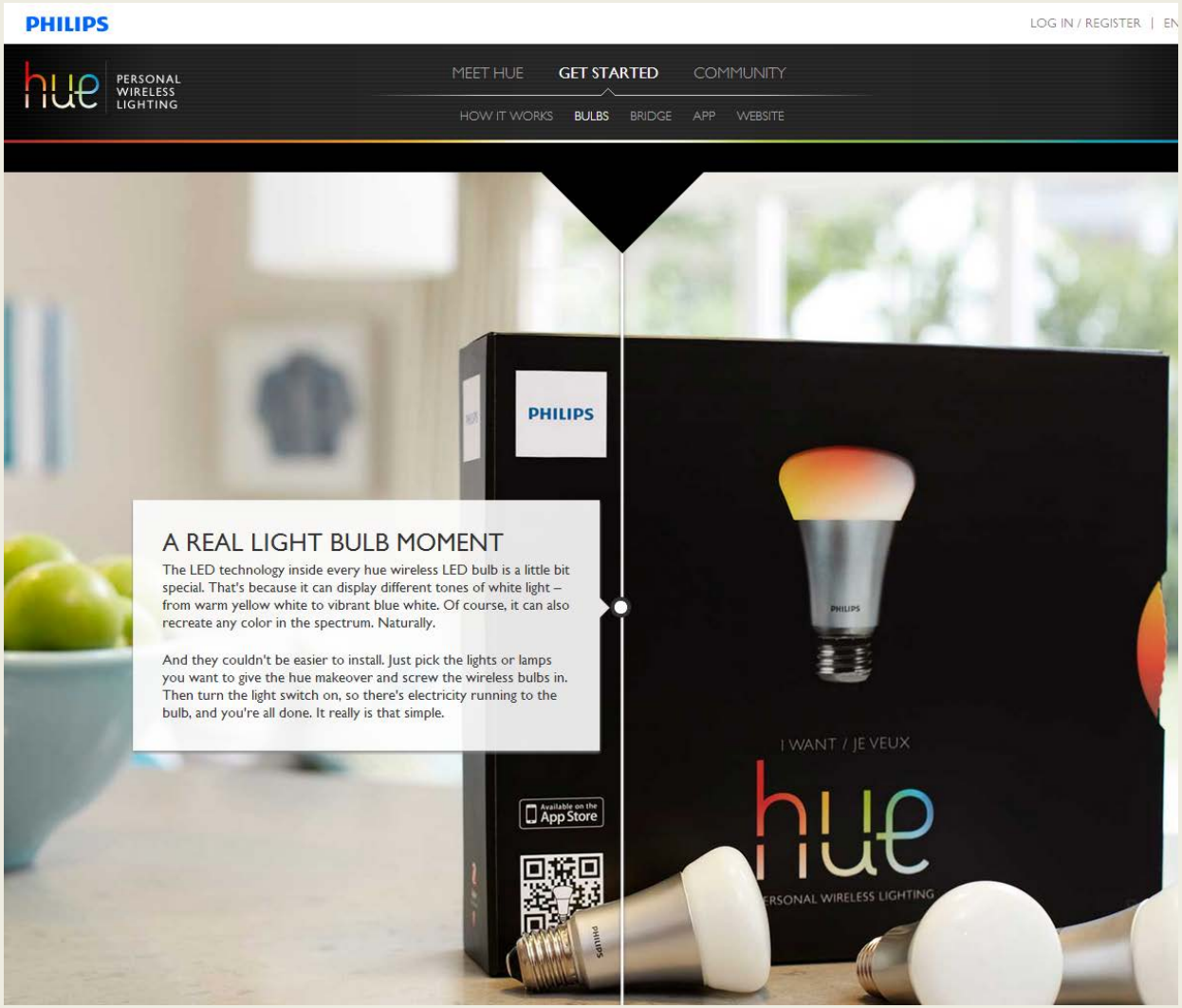
- ”vanlig” dator
- surfplatta, mobiltelefon
- tvspelskonsol, musikspelare, …
- kopieringsmaskin, annan kontorsutrustning

Var finns ”datorer” i samhället

- ”vanlig” dator
- surfplatta, mobiltelefon
- tvspelskonsol, musikspelare, …
- kopieringsmaskin, annan kontorsutrustning
- bil, flygplan, tåg (och system runt omkring)


000117 kWh

And even lamps need security



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

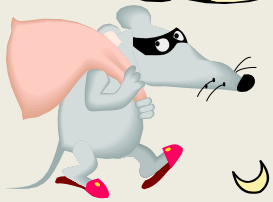
Var finns ”datorer” i samhället

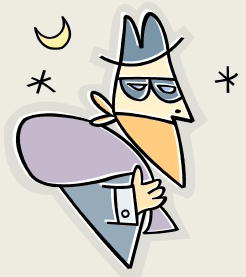
- ”vanlig” dator
- surfplatta, mobiltelefon
- tvspelskonsol, musikspelare, …
- kopieringsmaskin, annan kontorsutrustning
- bil, flygplan, tåg (och system runt omkring)
- samhällskritiska system: bankväsende, elförsörjning, transporter
- medicintekniska produkter: pacemaker …

Health care

Transportation

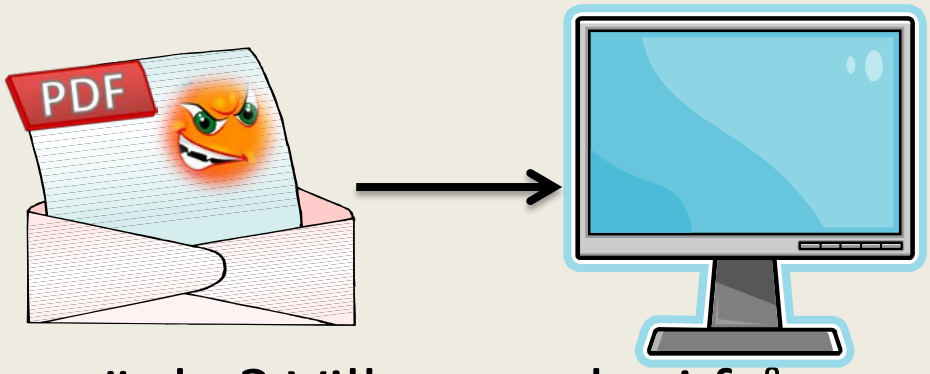
Financial



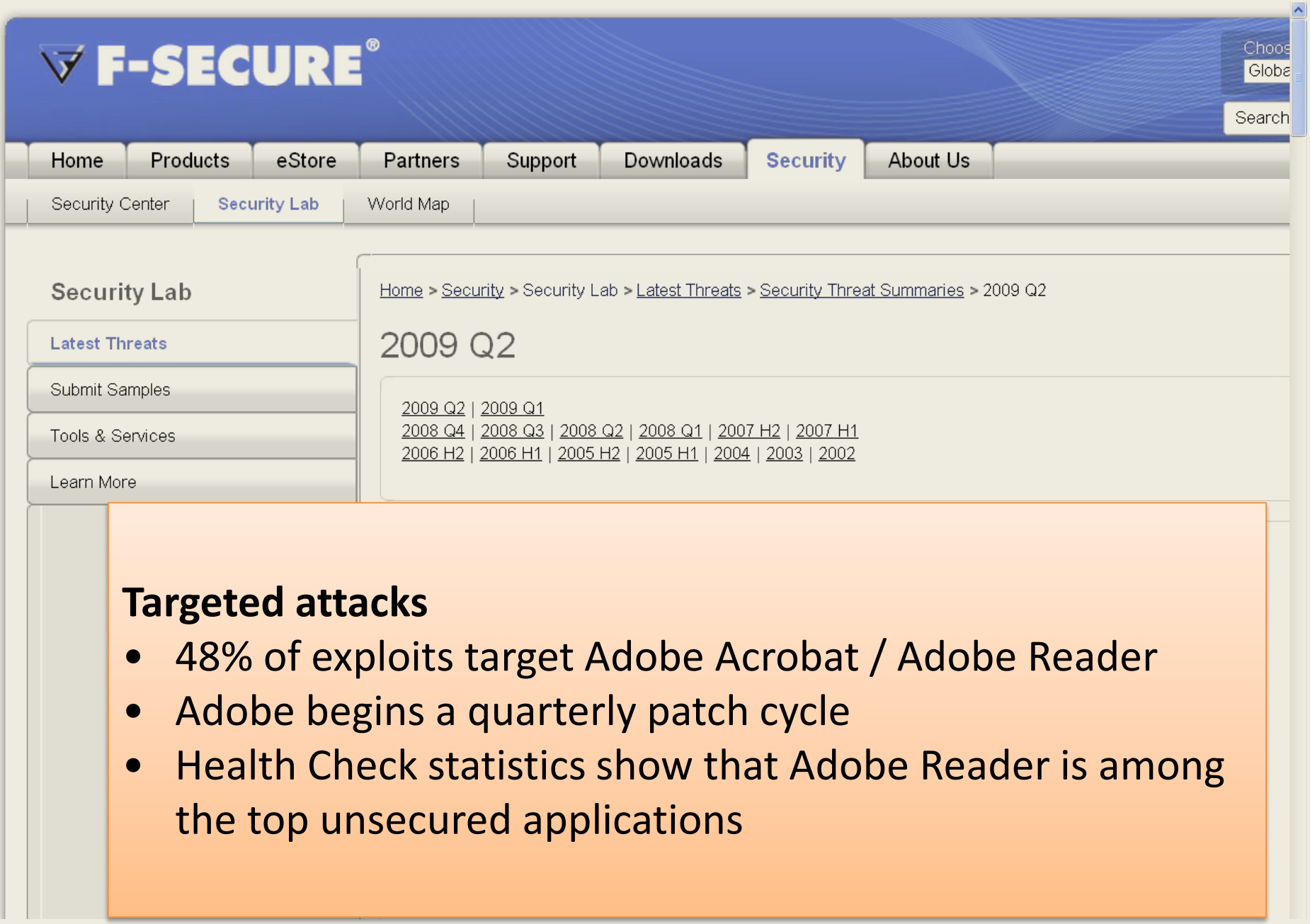


Skadlig kod

- **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

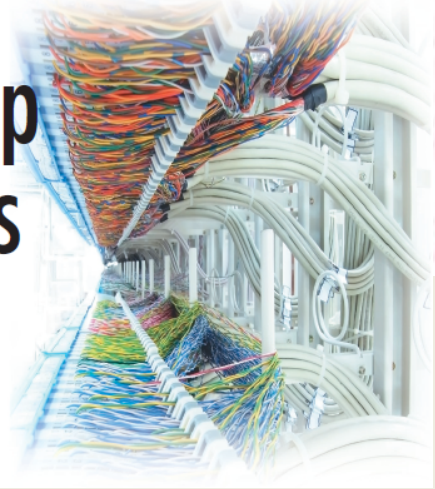
Uppdaterad: 2009-09-15 13:44

Datavirus på Kungälvs sjukhus

Ett föränderligt och svåråtkomligt datavirus har spridit sig på Kungälvs sjukhus. IT-teknikerna arbetar för högtryck med att begränsa skadorna.

TECHNOLOGY NEWS

Researchers Fight to Keep Implanted Medical Devices Safe from Hackers



Neal Leavitt

WIRED SUBSCRIBE » SECTIONS » BLOGS » REVIEWS » VIDEO » HOW

Sign In | RSS Feed

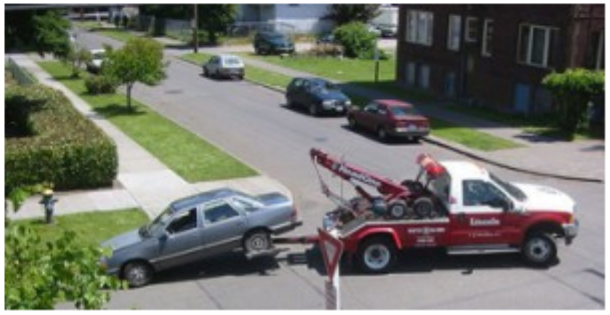
THREAT LEVEL

PRIVACY, 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



More than 100 drivers in Austin, Texas found their cars disabled or the horns honking out of control, after an intruder ran amok in a web-based vehicle-immobilization system normally used to get the attention of consumers delinquent in their auto payments.

Police with Austin's High Tech Crime Unit on Wednesday arrested 20-year-old Omar Ramos

ZDNet / News / Security

Malware link to air crash inconclusive

By Vivian Yeo, ZDNet Asia on August 30, 2010 (4 hours 44 minutes ago)

Summary

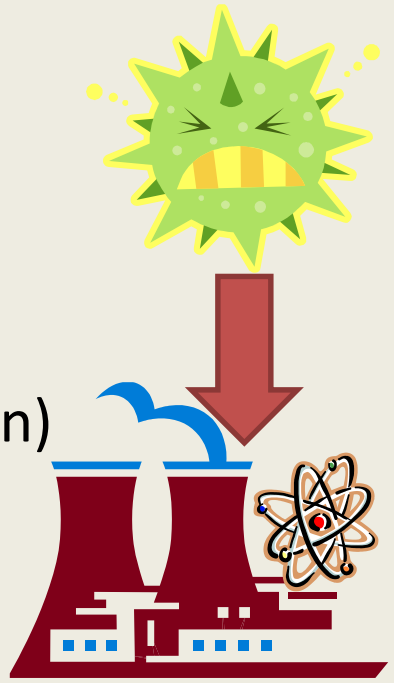
Although malware was recently identified as a contributing factor in years ago, it is still too early to draw definitive conclusions or panic cyberterrorism, security experts say.

Still too early to draw


THREAT LEVEL
smh.com.au
The Sydney Morning Herald
MEGA SHOW
PART 1
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

Ny tidsålder 2010: Stuxnet

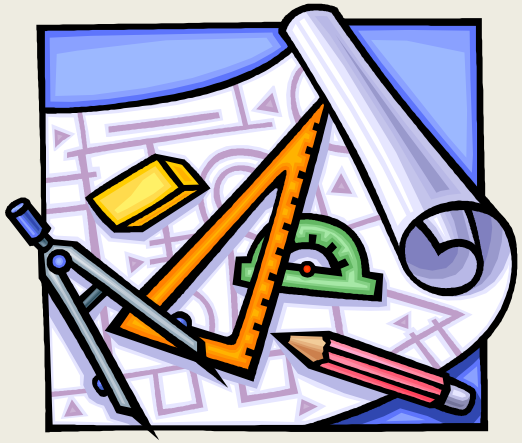
- Mycket avancerad skadlig kod
  - Med ett specifikt mål
    Programmerbara styrsystem:
    Siemens SIMATIC Step 7 software
  - Många rykten om mål och skapare
    - konstruerat av en stat
    - **Måltavla**: Kärnkraftverk i Bushehr, Iran
      (60% av alla stuxnet-infekterade datorer i Iran)



Symantec oct-2010: W32.Stuxnet Dossier (http://goo.gl/pP7S)

Stuxnet: Pandoras ask?

- Avancerat och ett av de första programmen som är konstruerat för att smitta styrsystem.
  - Det tog antagligen 6—8 personer ung 6 månader att skapa programmet.
- Styrsystem finns i många industrier
  - Monteringslinjer i fabriker, nöjesparker, belysningsarmatur



Nu existerar en ritning för skadlig kod mot styrsystem

- Jämför detta med viruset *Loveletter* (2000)
  - 2003/11 fanns det 82 olika varianter av detta virus
  - Fortfarande påstås det att mer än 5000 attacker per dag sker.

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

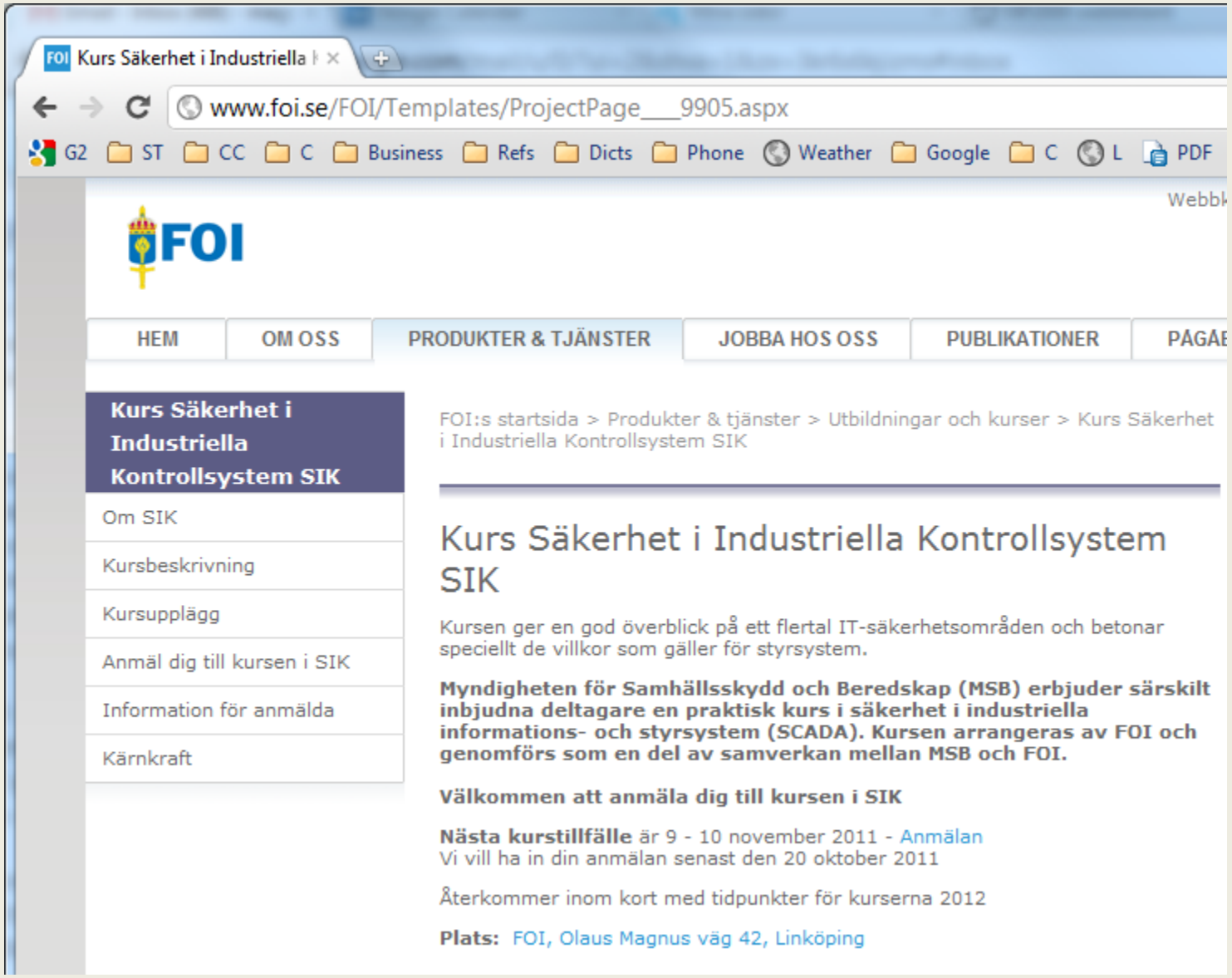
- Säkerhet är alltid en balansgång
- Vad vill man skydda? Till vilket pris?
- Några konkreta råd
  - Uppdatera systemet
  - Uppdatera alla program
  - Använd antivirus
  - Använd en brandvägg
  - Fundera på lösenorden
- Krypterad kommunikation viktig, mer behövs(!)

Forskning

- Detektering av ”botnets”
- Algoritmer för smarta elnät
- Bättre filtrering av skräppost
- Säkrare bilar
- Men även bättre stöd för att bygga komplicerade system.

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


Kurs Säkerhet i Industriella
www.foi.se/FOI/Templates/ProjectPage___9905.aspx
G2 ST CC C Business Refs Dicts Phone Weather Google C L PDF
FOI
HEM
OM OSS
PRODUKTER & TJÄNSTER
JOBBA HOS OSS
PUBLIKATIONER
Kurs Säkerhet i Industriella Kontrollsystem SIK
Om SIK
Kursbeskrivning
Kursupplägg
Anmäl dig till kursen i SIK
Information för anmälda
Kärnkraft
FOI:s startsida > Produkter & tjänster > Utbildningar och kurser > Kurs Säkerhet i Industriella Kontrollsystem SIK
Kurs Säkerhet i Industriella Kontrollsystem SIK
Kursen ger en god överblick på ett flertal IT-säkerhetsområden och betonar speciellt de villkor som gäller för styrsystem.
Myndigheten för Samhällsskydd och Beredskap (MSB) erbjuder särskilt inbjudna deltagare en praktisk kurs i säkerhet i industriella informations- och styrsystem (SCADA). Kursen arrangeras av FOI och genomförs som en del av samverkan mellan MSB och FOI.
Välkommen att anmäla dig till kursen i SIK
Nästa kurstillfälle är 9 - 10 november 2011 - Anmälan
Vi vill ha in din anmälan senast den 20 oktober 2011
Återkommer inom kort med tidpunkter för kurserna 2012
Plats: FOI, Olaus Magnus väg 42, Linköping

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

Security-related courses

The Computer Security is a basic and introductory course.
Other security-related courses in the CSN program are:

- Cryptography (TDA351) – sp 2
- Computer Security (EDA263) – sp 3
- Network Security (EDA491) – sp 4
- Language-based security (TDA601) – sp 4

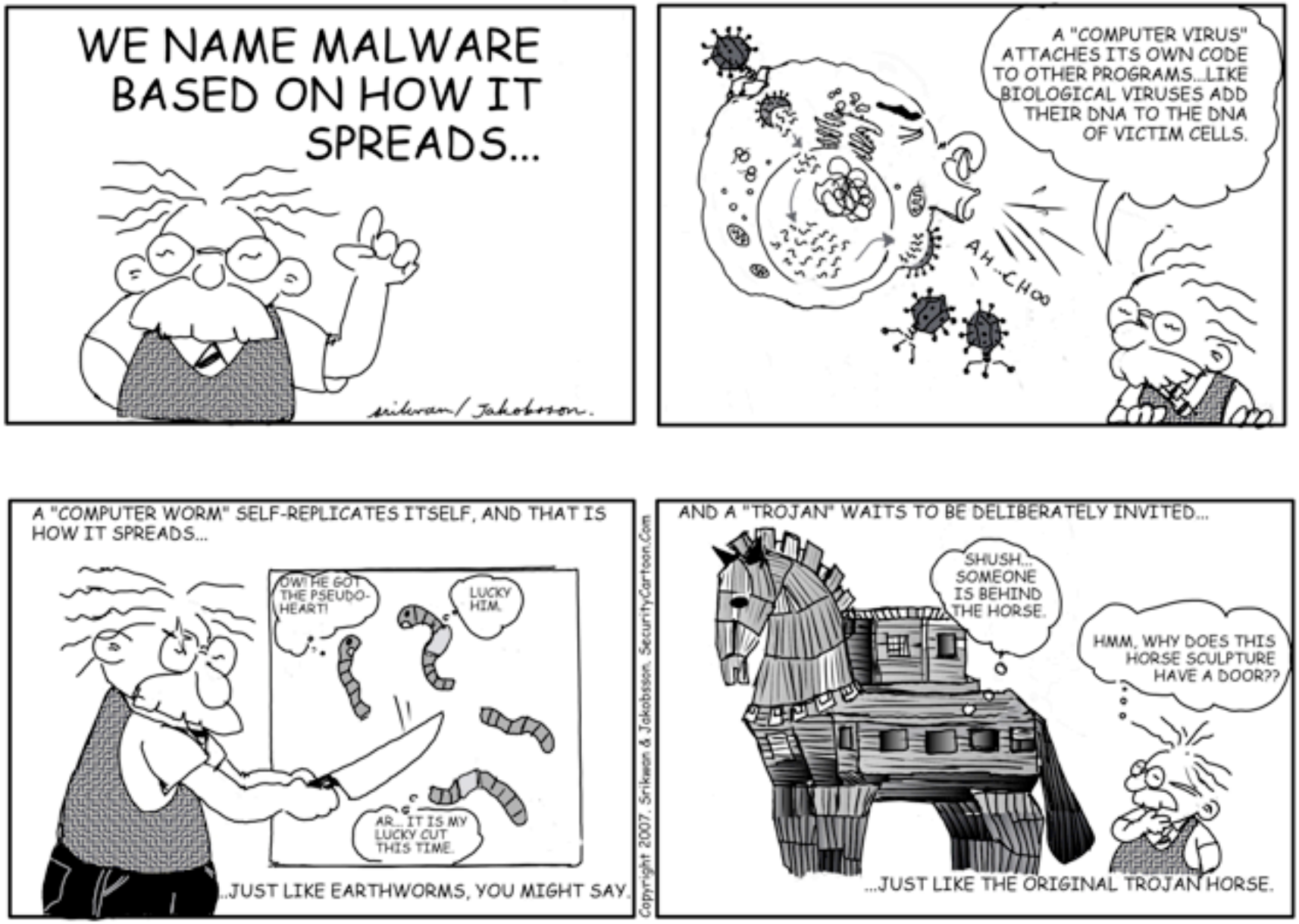
- *Project course: (sp 1)*
  ICT Support for Adaptiveness and Security in the Smart Grid (DAT300)

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

ICT SUPPORT FOR ADAPTIVENESS AND SECURITY IN THE SMART GRID



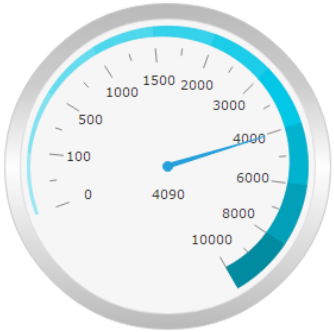
Competition
Capture the Flag

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!)