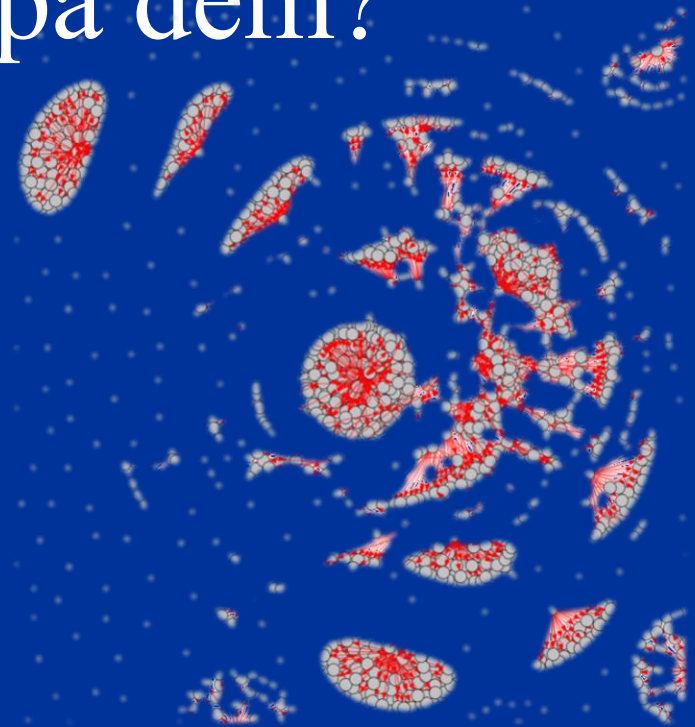


Datorer finns överallt, men kan man lita på dem?

Magnus Almgren

Göteborg 2019-04-01

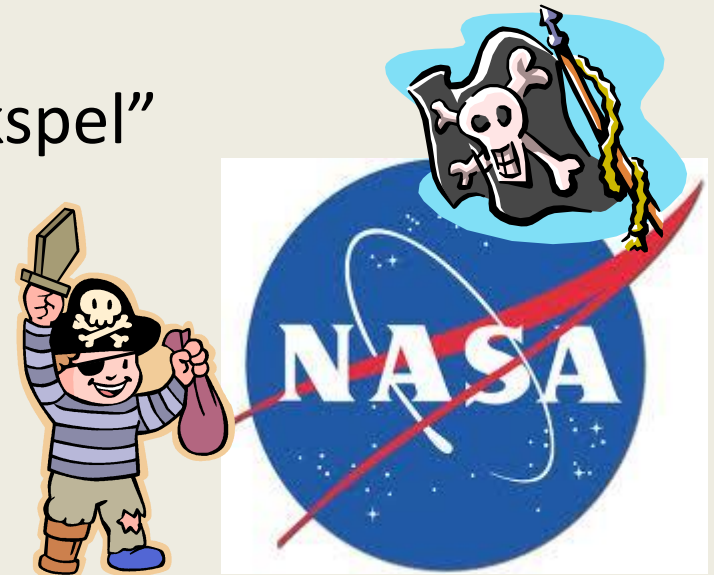


Security Quiz

- 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 överbelastningsattack mot IT-systemen.

M-Work


svt Trafikverket utreder IT-attacker

Secure | <https://www.svt.se/nyheter/inrikes/trafikverket-utreder-it-attack?lokal...>

Allt från SVT

svt NYHETER Lokalt

/ INRIKES



Haveriet innefattade bland annat att det automatiska systemet för att se var tågen befinner sig var utslaget. FOTO: TT

Trafikverket utreder IT-attack

Efter att tågtrafiken i hela Sverige drabbades av störningar och

Trafikverket nu utreda vad som kan ligga bakom. De misstänker att det beror på en överbelastningsattack mot IT-systemen.

Dagliga attacker ...

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

SVD Hackerattacker mot Väst

Secure | https://www.svd.se/hackerattacker-mot-vasttrafik?utm_source=SvDGBG1D&utm_medium=em

SVENSKA DAGBLADET > Start

Sverige

Hackerattacker mot Västtrafik

Västtrafik utsattes för hackerattacker under torsdagen. Bland annat uppträdde det ett stort problem med biljettköp.

Av Johanna Cederblad · 2 tim · Spara artikel · Dela



Under torsdagen var det problem med biljetter och annat i Västtrafiks system. Foto: Adam Ihse/TT



←  **Rocio**
last seen today at 11:53

Eller om det är komplicerat vi kan
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 📷 🎤

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?

Var finns "datorer" i samhället

- "vanlig" dator
- surfplatta, mobiltelefon
- TV-spel, musikspelare, ...



SUBSCRIBE >>

SECTIONS >>

BLOGS >>

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 a hacker intruder ran amok in a web-based vehicle-identification system normally used to get the state's consumers delinquent in their auto



Crime Unit on

- <https://youtu.be/MK0SrxBC1xs?t=72>

...override-malware/

'Crash Override': The Malware That Took Down a Power Grid

CULTURE

GEAR

IDEAS

SCIENCE

SECURITY

SHARE



SHARE
2316



TWEET



COMMENT



EMAIL

ANDY GREENBERG SECURITY 06.12.17 08:00 AM

'CRASH OVERRIDE': THE MALWARE THAT TOOK DOWN A POWER GRID



GETTY IMAGES

MOST POPULAR



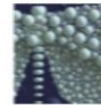
CULTURE
How 'The Matrix' Built a Bullet-Proof Legacy
BRIAN RAFFERTY



SECURITY
On the Trail of the Robocall King
ALEX W. PALMER



SPONSOR CONTENT
5 Questions with the Event Concierge Services Team
CONCIERGE.COM



SCIENCE
A Clever New Strategy for Treating Cancer, Thanks to Darwin
ROXANNE KHAMSI



MORE STORIES

AT MIDNIGHT, A week before last Christmas, hackers struck a major transmission station north of the city of Kiev,

the Ukrainian capital and

And even lamps need security

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



A close-up photograph of a person's hand holding a thin, flexible, silver-colored pacemaker lead wire. The wire is looped and held between the thumb and index finger. Overlaid on the hand and wire is a white, oval-shaped graphic containing text and a small image. The background is a blurred green lawn.

NEWS

Researchers Fight to Keep Implanted Medical Devices Safe from Hackers

Leavitt



Var finns "datorer" i samhället

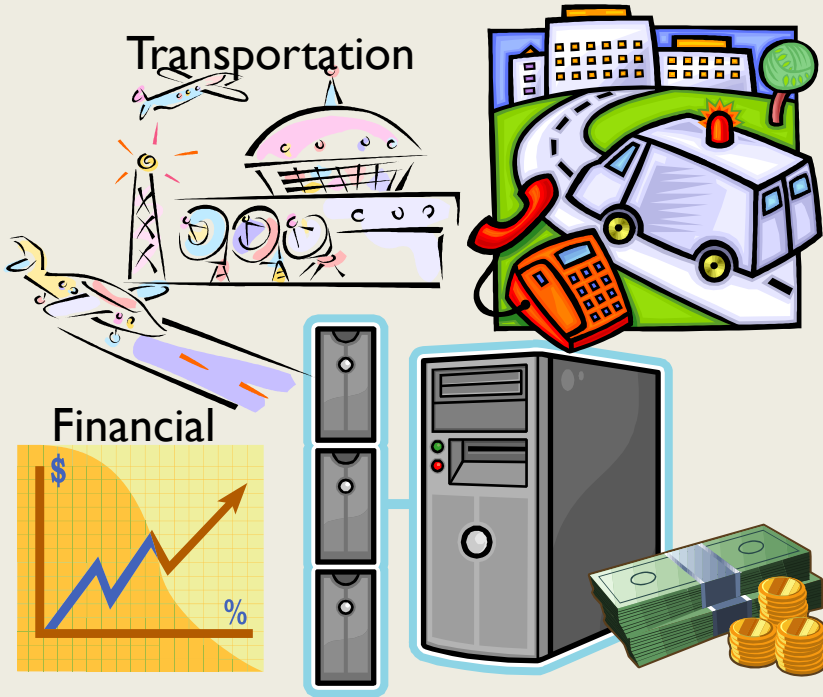
- "vanlig" dator
- surfplatta, mobiltelefon
- tvspelskonsol, musikspelare, ...
- kopieringsmaskin, annan kontorsutrustning
- bil, flygplan, tåg (och system runt omkring)
- samhällskritiska system: bankväsende, elförsörjning, transporter
- medicintekniska produkter: **pacemaker** ...

Internet of Things



Health care

Transportation





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.

280



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

PAID POST: THAI AIRWAYS
Find Frequent Flying Draining? Seasoned Filers Share Tips



Rohingya Refugees Fleeing Myanmar Await Entrance to Squalid Camps

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

繁體中文 | 繁體中文

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.”

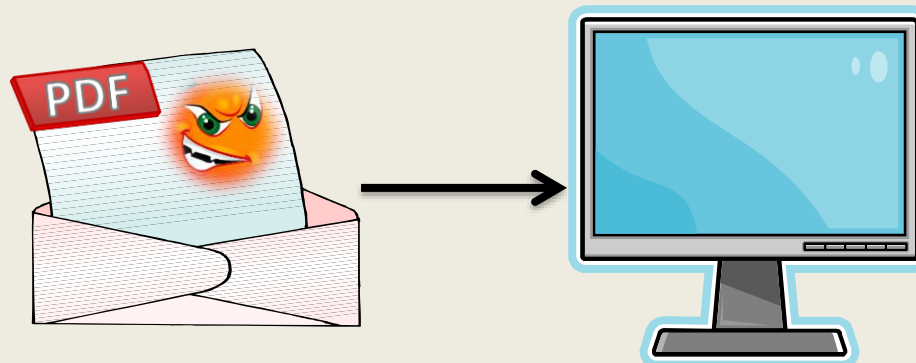
RELATED COVERAGE



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?

Security Lab

Latest Threats

[Submit Samples](#)[Tools & Services](#)[Learn More](#)

[Home](#) > [Security](#) > [Security Lab](#) > [Latest Threats](#) > [Security Threat Summaries](#) > 2009 Q2

2009 Q2

[2009 Q2](#) | [2009 Q1](#)[2008 Q4](#) | [2008 Q3](#) | [2008 Q2](#) | [2008 Q1](#) | [2007 H2](#) | [2007 H1](#)[2006 H2](#) | [2006 H1](#) | [2005 H2](#) | [2005 H1](#) | [2004](#) | [2003](#) | [2002](#)

Targeted attacks

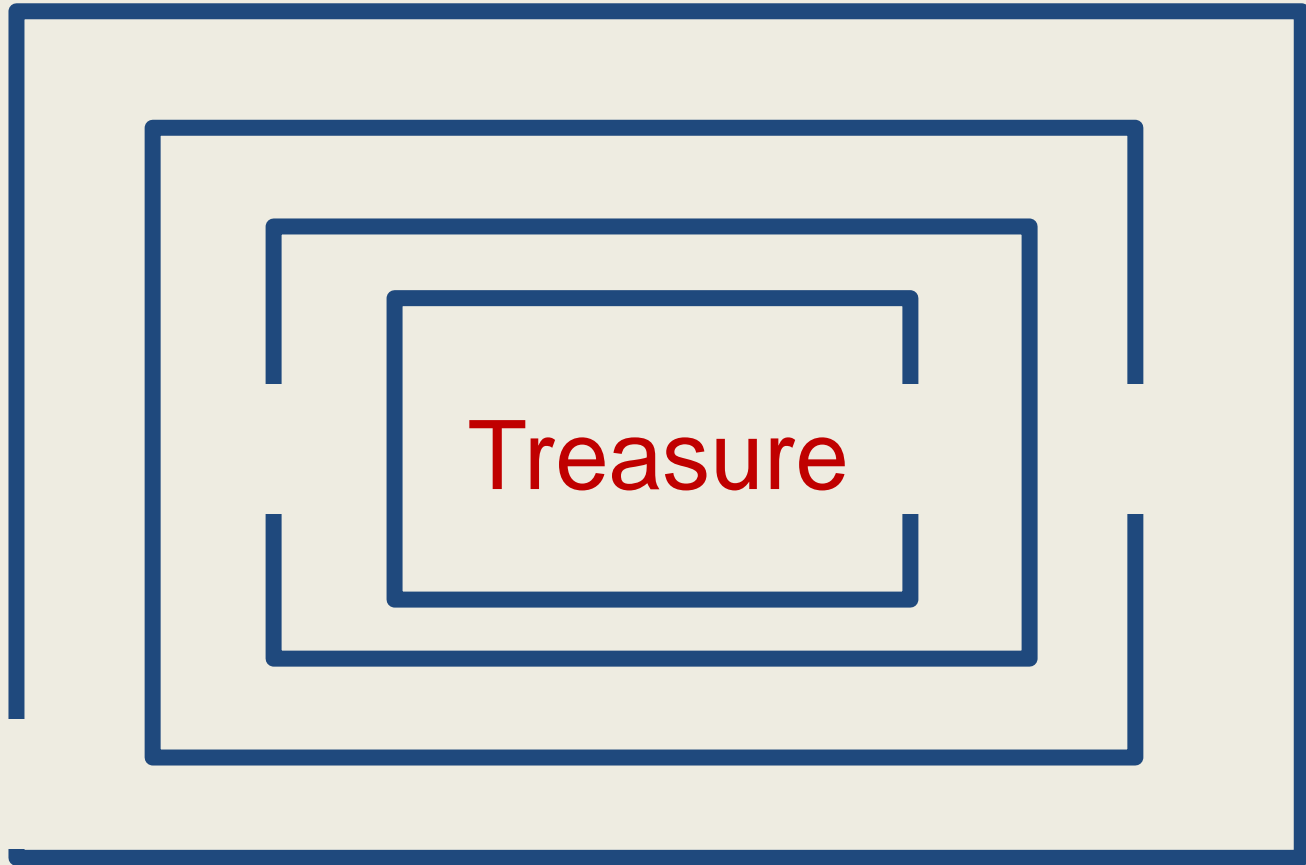
- 48% of exploits target Adobe Acrobat / Adobe Reader
- Adobe begins a quarterly patch cycle
- Health Check statistics show that Adobe Reader is among the top unsecured applications

Dangerous People (!!!)



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





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")**

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
 - Fundera på lösenord: ~~password~~ → passphrase, 2FA
 - Uppdatera systemet, alla program
 - Använd antivirus
 - Använd en brandvägg
- Krypterad kommunikation viktig, mer behövs(!)

Alla e-tjänster

Om e-legitimation

Har du tekniska problem med e-tjänster

Skatteverkets app

Mina sidor

Digital brevlåda


Blanketter

Broschyrer

Svar på vanliga frågor

Viktiga datum

Privat » Självservice » Alla e-tjänster » Spärra obehörig adressändring

 Lyssna

Spärra obehörig adressändring

Med e-tjänsten Spärra obehörig adressändring kan du förhindra att någon obehörig ändrar din adress. När spärren är aktiverad godkänns bara adressändringar som görs med e-legitimation i Skatteverkets e-tjänster för Flyttanmälan eller Särskild postadress. Detta minskar risken för att någon använder dina personuppgifter för bedrägerier och id-kapning. Spärr av obehörig adressändring kan bara göras via den här e-tjänsten.

Det här kan du göra

- spärra obehörig adressändring genom att bara tillåta ändringar som görs med e-legitimation
- ta bort spärren för obehörig adressändring genom att även tillåta ändringar som görs på blankett.

Vem kan använda e-tjänsten?

- E-tjänsten kan bara användas av privatpersoner. Den kan alltså inte användas av företag.
- Du måste ha fyllt 18 år för att använda e-tjänsten.
- När du har spärrat för obehörig adressändring kan familjemedlemmar som är folkbokförda tillsammans med dig fortfarande ändra din adress om de använder e-legitimation. Exempel på familjemedlemmar är make, maka, registrerad

Logga in till e-tjänsten

Inloggning >

Öppettider: 00-24

Relaterade e-tjänster

Flyttanmälan >

Särskild postadress >

Mobil e-legitimation

Använd [Mobilt BankID](#) för att logga in på din dator.

Eller om det är komplicerat vi kan 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  

Forskning

Industriella Kontrollsystem & Sakernas Internet



RIOT

Annan forskning

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

Doktorera? Kontakta oss tidigt och arbeta med oss!

Exjobb? Öka chanser för industrin?



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.





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

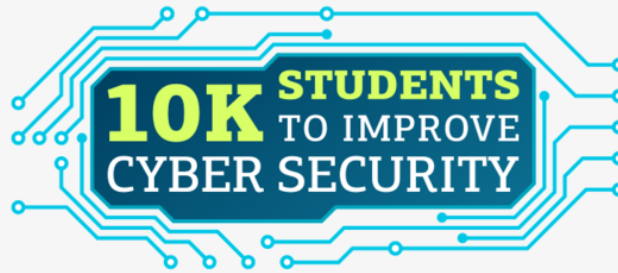
DATA-DRIVEN SUPPORT FOR CYBER- PHYSICAL SYSTEMS



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.



An Initiative of the **syssec** Consortium

About

Participants

Material

Join Us

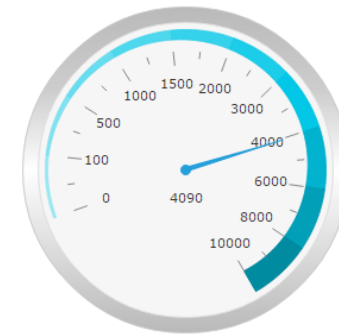
What is the 10KStudents Challenge?

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**..."*



+4 Recommend this on Google

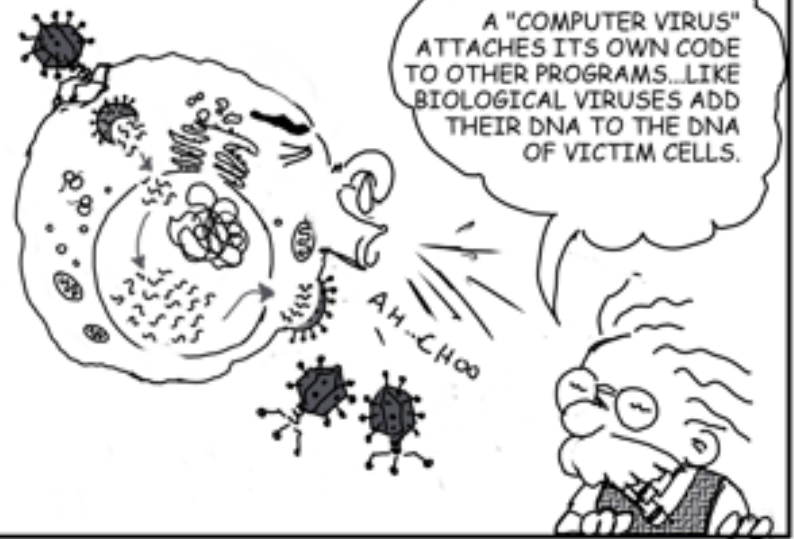
Like Share 15 people like this. Sign Up to see what your friends like.

WE NAME MALWARE
BASED ON HOW IT
SPREADS...

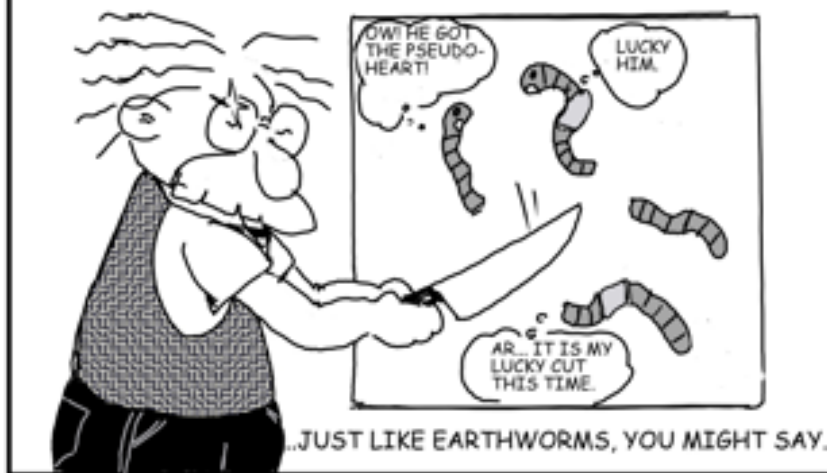


Srikaran/Jakobsson.

A "COMPUTER VIRUS"
ATTACHES ITS OWN CODE
TO OTHER PROGRAMS...LIKE
BIOLOGICAL VIRUSES ADD
THEIR DNA TO THE DNA
OF VICTIM CELLS.



A "COMPUTER WORM" SELF-REPLICATES ITSELF, AND THAT IS
HOW IT SPREADS...



...JUST LIKE EARTHWORMS, YOU MIGHT SAY.

AND A "TROJAN" WAITS TO BE DELIBERATELY INVITED...



...JUST LIKE THE ORIGINAL TROJAN HORSE.

Copyright 2007, Srikaran & Jakobsson, SecurityCartoon.Com