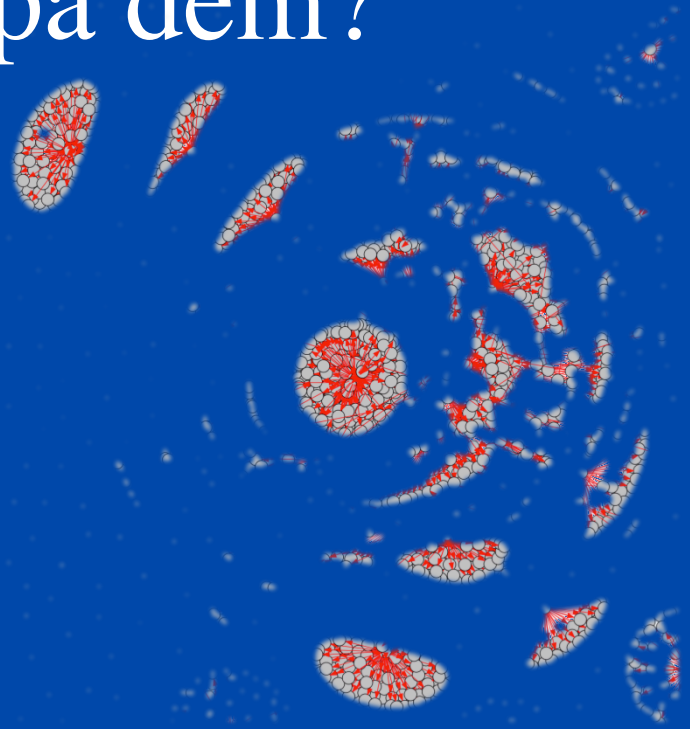
Datorer finns överallt, men kan man lita på dem?

Magnus Almgren

Göteborg 2011-05-11



Postdoc, finansierad av MSB

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 som hemanvändare?
- Vad sker inom forskningen?

Ett europeiskt nätverk för att studera hot och svagheter i framtidens internet

- "Network of Excellence" (2010-2014)
- För att arbeta mot lösningar och samarbeta
  - På europeisk nivå
    - Poli. di Milano (IT)
    - Vrije Uniivesriteit (NL)
    - Institute Eurecom (FR)
    - IPP (Bulgaria)
    - TU Vienna (Austria)
    - Chalmers U (Sweden)
    - UEKAE (Turkey)
    - FORTH – ICS (Greece)
  - och med internationella kollegor i hela världen

Var finns ”datorer” i samhället

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


Hack-att 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)


kWh

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 …

och vilka är angriparna?

- Kriminella nätverk
- Företag för industrispionage
- Grupper med en gemensam politiskt agenda eller annan gemensam övertygelse
- Terrorister
- Fientligt inställda länder (via militären?)
- Tonåringar?

Organisationer med vitt skilda mål

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?
  - Surfa på webben?

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

Ett par exempel på attacker 2010

- Google attackeras
- Forskare visar att medicintekniska produkter kan attackeras
- Dator på flygplats infekteras med skadlig kod
- Missnöjd före detta anställd stänger av bilar
- Virus nära att spridas till energisystem
- Estland attackeras av en *DoS* attack (2007)

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)

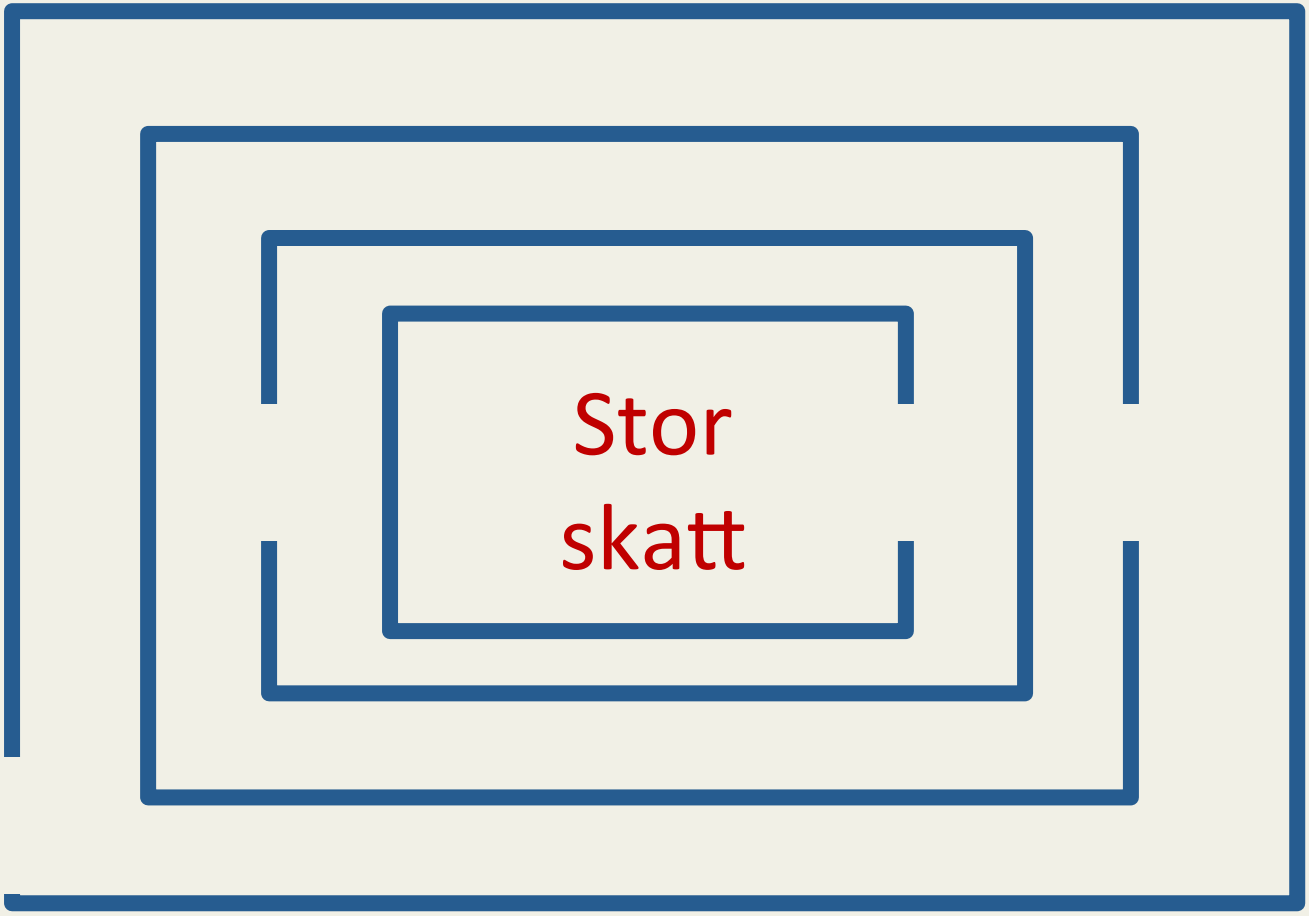
Stuxnet: Pandoras ask?

- 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.

Förklaring av datorattacker



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”)
- TOCTOU-attack = kontrollen sker inte när filen används

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

Hemanvändare

- 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

Hacker-tävling: pwn2own

- Hackers får betalt om de lyckas infektera en dator genom webbläsaren (ung 100,000 kr)
- Förekommit flera år i rad
- Hittills har bara Googles webbläsare lyckats stå emot angriparna varje år
- Men tävlingen säger inget om en webbläsare egentligen är säker
  - Kanske spar man på attacken för att få en större prissumma?
  - Det beror mycket på hur man konfigurerar webbläsaren och vilka insticksprogram man använder.

Forskning

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

Länkar

- *SVT Dokumentär okt-2010:*
  - *Att hacka en stormakt (http://goo.gl/1Zrd)*
- *Symantec okt-2010:*
  - *W32.Stuxnet Dossier (http://goo.gl/pP7S)*
- *Uppdrag granskning okt-2010:*
  - *Kapade nätverk (http://svt.se/granskning)*
- *SysSec: http://www.syssec-project.eu/*