Hoten mot våra digitala system

Christer Åhlund
Prof. Distribuerade datorsystem
Möjliggörande IKT

LULEÅ
TEKNISKA
UNIVERSITET

Innehåll

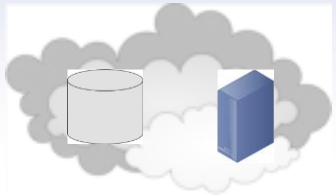
- **Introduktion**
- Kända attacker
- IKT-säkerhet
- En hackares arbetsmoment och verktyg
- Vad vet världen om dina system?
  - Ett exempel, Shodan

Ökat antal digitala miljöer = Digitalisering

- En intressant kombination av möjligheter…
- …men varje uppkopplat system mot Internet ökar dess utsatthet....
- ....så vi måste veta vad vi gör!

LULEÅ TEKNISKA UNIVERSITET

Teknologitrender



- Cyber-fysiska system
  - IKT som agerar i fysiska objekt
- Sakernas Internet
  - Ett Internet uppkopplat cyber-fysiskt system
- Öppen data
  - Fritt tillgänglig data utan inskränkning
- Molnplattformar
  - <*x*>-as as service

The “Internet Security Threat Report 2019”

- Av Symantec
  - https://www.symantec.com/security-center/threat-report
- ”Key findings”
  - Formjacking attacks skyrocketed, with an average of 4,800 websites compromised each month.
  - Ransomware shifted targets from consumers to enterprises, where infections rose 12 percent.
  - More than 70 million records stolen from poorly configured S3 buckets, a casualty of rapid cloud adoption.
  - Supply chains remained a soft target with attacks ballooning by 78 percent.
  - “Smart Speaker, get me a cyber attack” — IoT was a key entry point for targeted attacks; most IoT devices are vulnerable.

Innehåll

- Introduktion
- **Kända attacker**
- IKT-säkerhet
- En hackares arbetsmoment och verktyg
- Vad vet världen om dina system?
  - Ett exempel, Shodan

Kända attacker: Foscam-historien

- Webkamera
- Default username:admin, password:
- Senare gjordes en uppgradering som kräver att man sätter ett lösenord.
  - Uppgraderingen krävde manuell installation
  - En studie från (ett år efter uppdateringen), Exploiting-Foscam-IP-Cameras, visar på att ingen kamera som undersöktes hade den senaste programvaran installerad

N. Dhanjani, Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts. O'Rielly, 2015

Kända attacker: Foscam-historien (forts.)

- Dynamisk DNS används
  - En unik 6-teckens kod används, angiven på varje enhet, ex. aa0000-ep9310
  - Anger både användare och lösenord för DNS-tjänsten
  - Binder enhetsnamn xx####.myfoscam.org till den IP adress som används
- Möjligt hack?
  - En hacker använder ett namn slumpis, ex. ab0002 och skickar en uppdatering till DNS-systemet ns1.myfoscam.org, med slumvist valt namn som användare och lösenord
  - DNS-systemet uppdaterar bindningen till hackarens IP adress
  - Hackaren startar en webserver som ser ut som Foscamgränssnittet
  - Ägaren av kameran söker åtkomst till kameran via DNS och får lagrad IP adress som svar
  - Vid försök till kameraåtkomst så matas inloggningsinformationen in på hackarens hemsida, meddelande om felaktig användare/lösen fås
  - Hackaren återställer IP adressen till den riktiga kameran för att dölja intrånget
  - Nu är kameran nåbar för hackaren (så länge användarnamn och lösenord inte ändras)

N. Dhanjani, Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts. O'Rielly, 2015

Kända attacker

- Intrång i Webbdatorcentralens styrsystem för fastigheter
  - Låg säkerhet vid inloggning
  - Remote kontroll av exempelvis värme, låssystem, brandlarm med mera

Kända attacker

- Dyn cyberattack, en DDOS attack mot DNS leverantören Dyns system.
  - 1.2 Tbit/s
  - Använde sakernas Internet infekterade med Mirai (Botnet attack)

Kända attacker

- Keen security lab hackar Tesla modeller
  - Åtkomst till CAN-bussen
  - Kunde kontrollera bilen på distans

Innehåll

- Introduktion
- Kända attacker
- **IKT-säkerhet**
- En hackares arbetsmoment och verktyg
- Vad vet världen om dina enheter?
  - Ett exempel, Shodan

Digitalisering….

- Det krävs att vi kan
  - Säkerställa källan som skapar data/information
  - Validera korrekthet i data/information
  - Skydda data/information från obehörig åtkomst
  - Tillhandahålla tillgänglighet

Behov av IKT-säkerhet

- Skydd av datorsystem från stöld och förstörelse av hård och mjukvara samt information

Behov av IKT-säkerhet

- Autentisering
  - Skaparen av data/information och validering av dess originalitet
  - Åtkomsträttigheter till system samt data och information
- Konfidentialitet
  - Endast tolkningsbart för behöriga

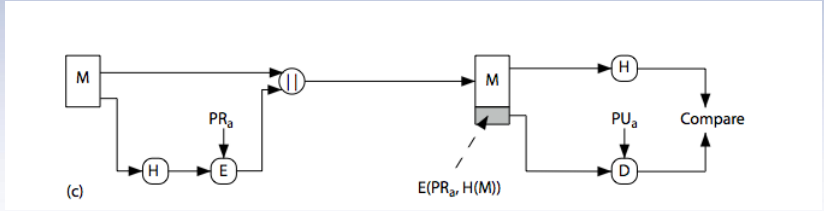
LULEÅ TEKNISKA UNIVERSITET

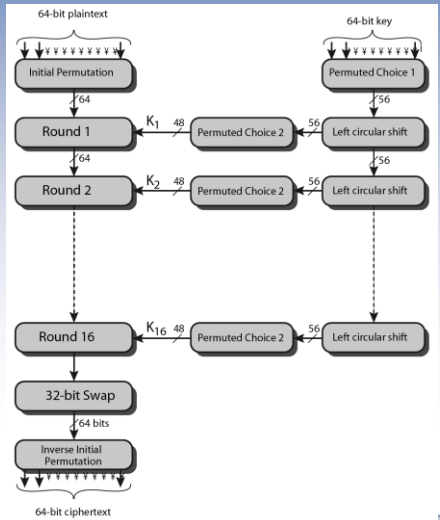
Behov av IKT-säkerhet

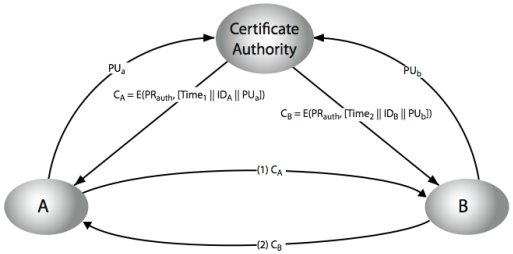
- Integritet
  - Information som kan vara skadlig för individ och organisation skyddas
- Tjänstetillgänglighet
  - Åtkomst till nätverk, servrar (DNS, molnplattformar, m.m)

Följande krävs

- Kryptering
  - AES, RSA
- Autentisering
  - Hash, MAC för information
  - Lösenord för accesskontroll
- Hantering av nycklar
  - Symmetriska, asymmetriska
  - $K_{AB} = a^{x_A . x_B} \bmod q$







Bildern är från *Cryptography and Network Security*, W. Stallings

LULEÅ TEKNISKA UNIVERSITET

Skydd av algoritmer och nycklar

- Algoritmerna som används inom IKT-säkerhet ska anses som öppna
  - Initialt så försökte dessa hemlighållas men information läckte ofta ut

Exempel:RSA

Skapa RSA nycklar

1. Välj primtal, ex: $p=17$ & $q=11$
2. Beräkna $n = pq = 17 \times 11 = 187$
3. Beräkna $\phi(n)=(p-1)(q-1)=16 \times 10=160$ (Euler's totient funktion)
4. Välj e: $\gcd(e,160)=1$; ger $e=7$
5. Bestäm d: $de=1 \bmod 160$ och $d < 160$ ger $d=23$ då $23 \times 7=161= 10 \times 160+1$ (Euler's teorem)
6. Publik nyckel $PU=\{7,187\}$
7. Privat nyckel $PR=\{23,187\}$

Enkel RSA kryptering/dekryptering

1. Givet meddelande $M = 88$ (nb. $88<187$)
2. Kryptering:
   - $C = 88^7 \bmod 187 = 11$
3. Dekryptering:
   - $M = 11^{23} \bmod 187 = 88$

LULEÅ TEKNISKA UNIVERSITET

Skydd av algoritmer och nycklar

- Algoritmerna som används inom IKT-säkerhet ska anses som öppna
  - Initialt så försökte dessa hemlighållas men information läckte ofta ut
- Nycklarna är *nyckeln* till säkerhet
  - Kräver god hantering och lägger ansvaret på systemadministrationen och användare

Konklusion

- Val av lämplig algoritm och hantering av nycklar är avgörande
  - Tid för hur länge något ska vara säkert är också viktigt att ta hänsyn till

Innehåll

- Introduktion
- Kända attacker
- IKT-säkerhet
- **En hackares arbetsmoment och verktyg**
- Vad vet världen om dina system?
  - Ett exempel, Shodan

Arbetsmoment för en hacker

- Skapa förutsättningar för att vara anonym
  - Ex. Proxychains, VPN
- Samla information (foot printing)
  - Ex. “who is”, nslookup, nmap
- Intrång
  - Ex. “John The Ripper”, Hydra
- Förändra systemfunktion, inhämta information
  - Ex. installation av Malware
- (Dölj spåren efter intrånget)

Några typer av attacker

- Malware(sabotageprogram)
  - Virus, maskar, trojansk häst, spionprogram, ransomware, cross-site scripting (XSS)
- Nätfiske
- Att använda *bakdörrar*
- DDOS
- Vid åtkomst till en fysisk enhet kan ex. JTAG användas för att komma åt processor, minne och andra enheter för att komma åt känslig information

Åtkomst till system på plats

- Trådlös kommunikation
  - Z-Wave
    - Security Evaluation of the Z-Wave Wireless Protocol
  - Zigbee
    - Zigbee exploited
  - WiFi
    - DoS attack för att tvinga fram ny autentisering – sänd deauhentication request, inspektera autentiserings proceduren.
    - Hacka PIN autentisering (WPS) med ex. Reavers

Åtkomst till system på distans (forts.)

- Exempel på standardportar
  - SSH(port 22)
  - Webtjänster (port 80)
  - SNMP (port 161)
  - M.fl.
- Kombinationer av öppna portar kan informera om vilket operativsystem som används
- HTTP-Server fältet innehåller information som möjliggör att identifiera enheter/tjänster

En palett av verktyg

- Kali Linux

Innehåll

- Introduktion
- Kända attacker
- IKT-säkerhet
- En hackares arbetsmoment och verktyg
- **Vad vet världen om dina system?**
  - **Ett exempel, Shodan**

Shodan

- www.shodan.io
- Shodan läser av banner-fält, ex.
  - HTTP/1.1 200 OK
  - Server: nginx/1.1.19
  - Date: Sat, 03 Oct 2015 06:09:24 GMT
  - Content-Type: text/html; charset=utf-8
  - Content-Length: 6466
  - Connection: keep-alive
- Även metadata såsom
  - Datornamn
  - Geografiskt läge
  - Operativsystem
  - M.fl.

Shodan

- Sökalgoritm
  1. Skapa en slumpvis IP address
  2. Slumpa portnummer
  3. Se om en banner kommuniceras vid uppkoppling
  4. Goto 1

Några möjligheter med Shodan

- Hitta hackade hemsidor som har titeln ”Hacked by” i Sverige
  - http.title:xxxx country:xx
- Hur många servrar i Sverige är inte uppdaterade för att motstå Heartbleed buggen?
  - Tips,hitta identifikation på http://cve.mitre.org/
  - vuln:##...# country:xx (ssl.version:)

Några möjligheter med Shodan

- Finn de industriella styrsystemen (ics) i din kommun
  - category:ics city:xxx…xx
- Hur många nationella VNC servrar tillåter anonym access?
  - rfb authentication disabled country:se

Frågor