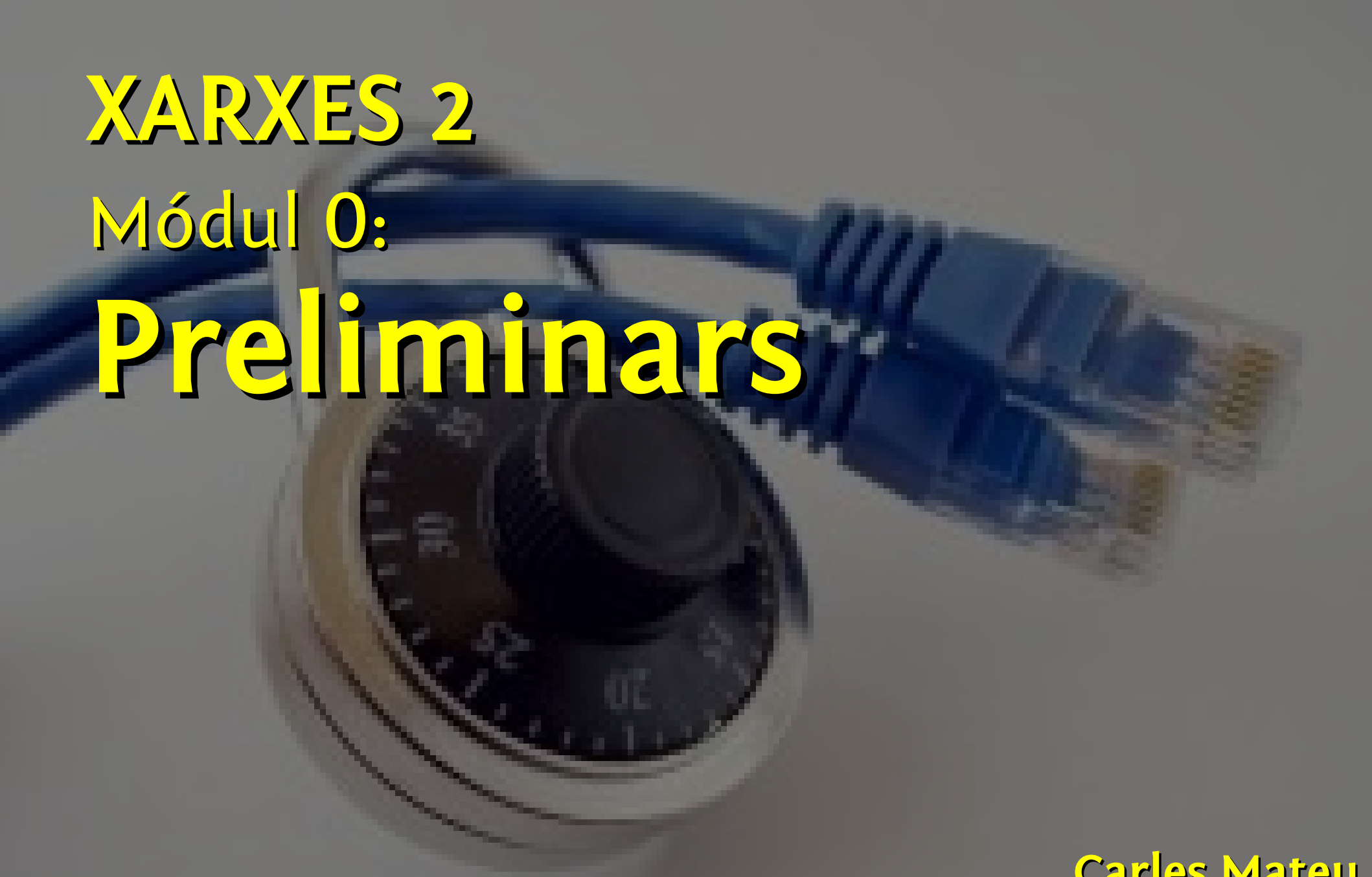
XARXES 2

Mòdul 0:

Preliminars



Carles Mateu
Departament d'Informàtica i Enginyeria Industrial
Universitat de Lleida

Objectius

Conéixer els fonaments de la seguretat i la inseguretat informàtica.

Aprendrem:

- Vocabulari bàsic de seguretat.
- Tipus de problemes possibles.
- Finalitat de la seguretat informàtica.

Objectius Seguretat

La seguretat de les TI té 4 objetius fonamentals:

- Confidencialitat
- Integritat
- Disponibilitat
- Legitimitat

Defincions

Confidencialitat

Protecció de la informació preservant-la de revelació accidental o no dessitjada:

- Impedint-ne l'accés
- Fent-la ininteligible en cas d'accés

Defincions

Integritat

Protegir la informació d'alteracions i modificacions no permeses o dessitjades.

Defincions

Disponibilitat

Confiabilitat i capacitat de la xarxa/sistema de recuperar-se completament de caigudes i interrupcions de servei.

Defincions

Legitimitat

Abilitat i capacitat de controlar l'accés als recursos, permetent accés als recursos legítims i denegant-lo en altre cas.

Disciplines

La seguretat de les TI :

- Seguretat de comunicacions
- Seguretat de Sistemes

Altres:

- Seguretat física
- Seguretat administrativa/personal
- etc.

Conceptes bàsics

Política de seguretat

Conjunt de regles i procediments establerts per aplicar-se a totes les activitats d'un domini de seguretat.

Conceptes bàsics

Autenticació

Validar i donar per vàlida (auténtica) l'identitat d'algú o d'alguna cosa.

Conceptes bàsics

Autorització

Garantir uns drets, que estabiliran **qui** pot fer el **que** a quin **objecte**.

Conceptes bàsics

Comptabilitat (Accounting)

Registre de les activitats realitzades per algú

Conceptes bàsics

Amenaça (Threat)

Persona, cosa, idea o event que posa en perill la seguretat d'un recurs.

Conceptes bàsics

Atac

Realització efectiva d'una amenaça de seguretat, generalment de forma deliberada.

- **Passiu**: no altera informació.
- **Actiu**: altera informació.

Conceptes bàsics

Vulnerabilitats

Situacions de feblesa o d'absència de salvaguardes.

Conceptes bàsics

Salvaguardes

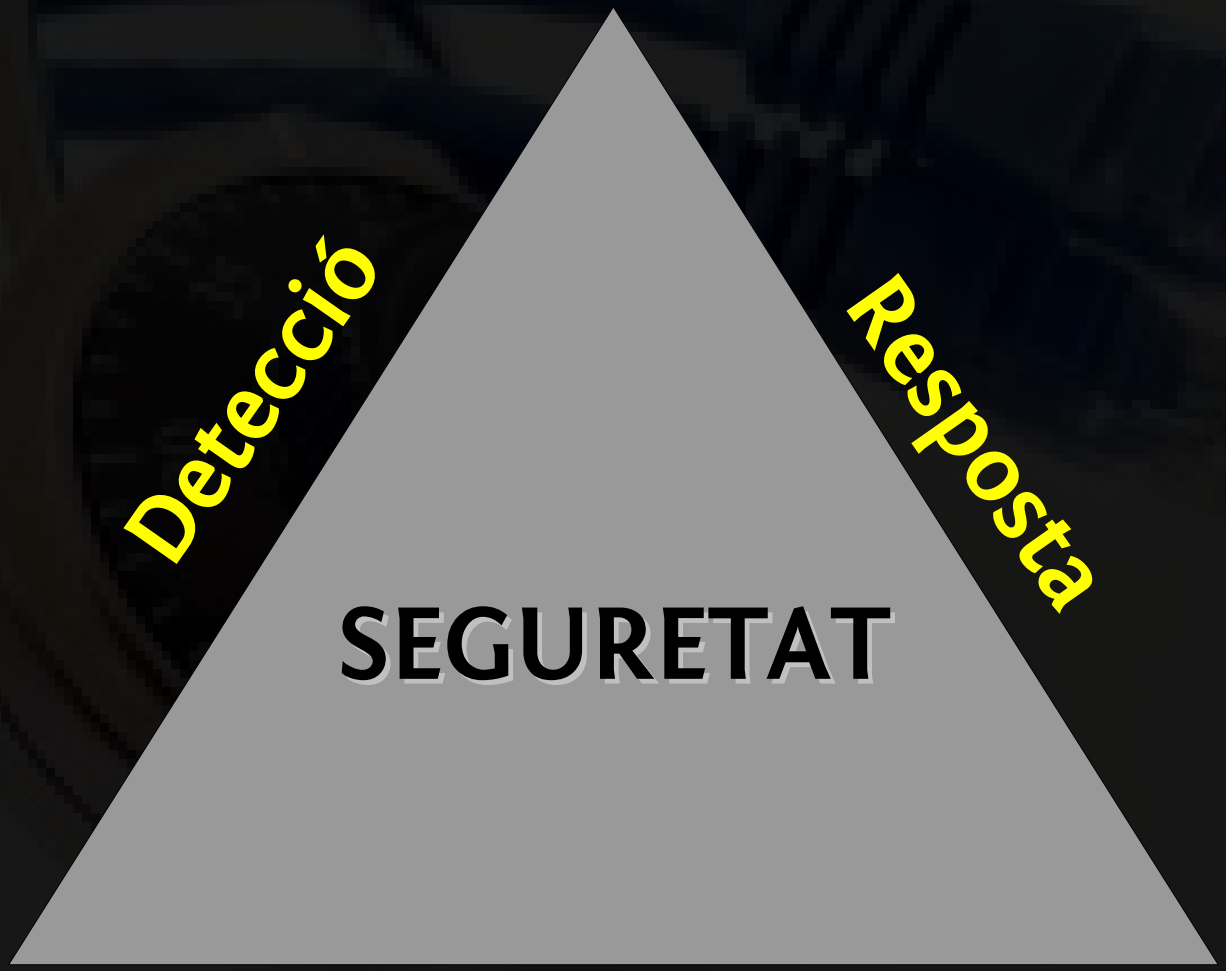
Mecanismes, polítiques i procediments de protecció, destinats a evitar, retardar o detectar atacs.

Conceptes bàsics

Risc

Cost estimat d'una vulnerabilitat, tenint en compte la probabilitat que un atac tingui èxit.

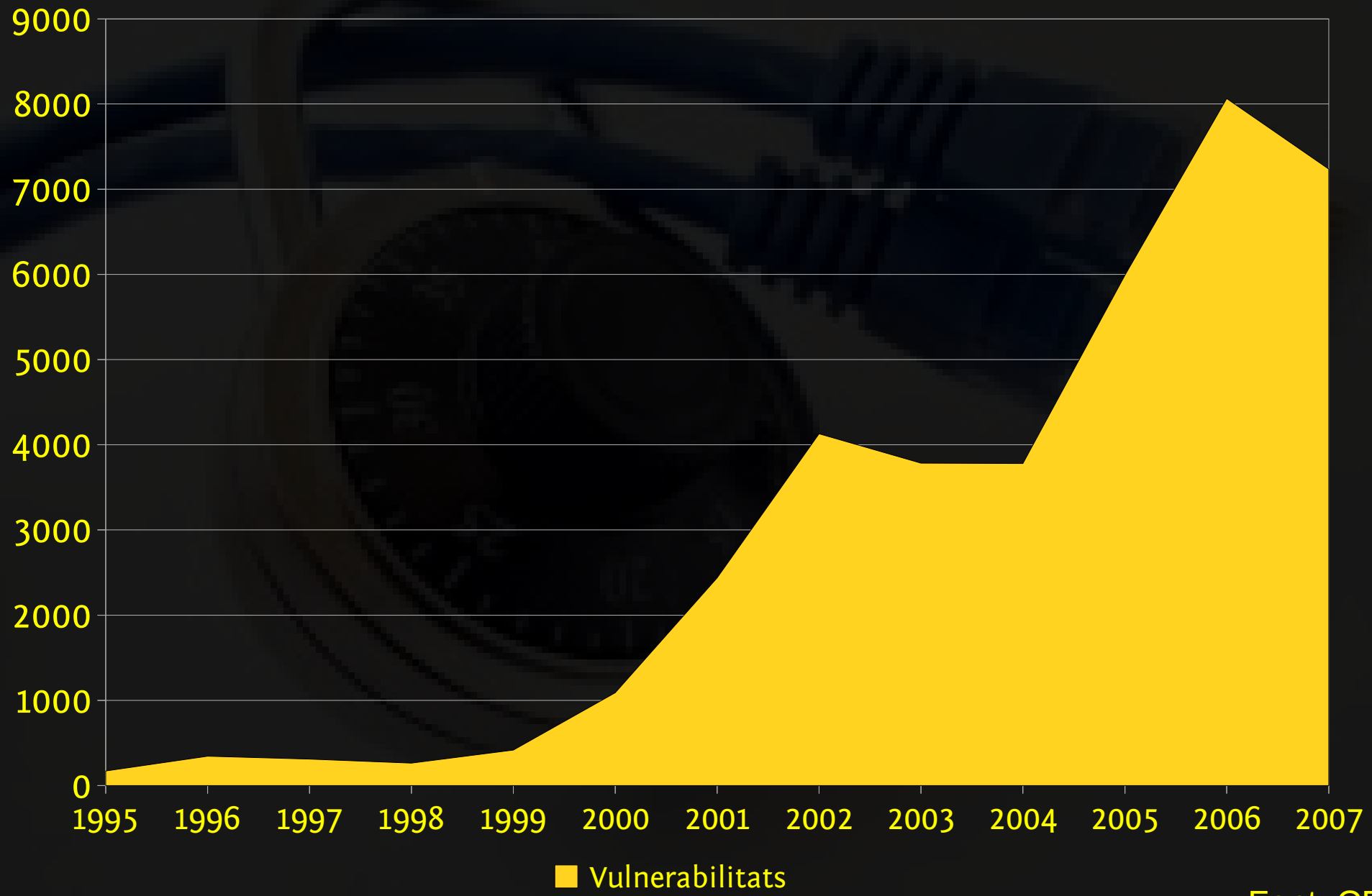
Trinitat seguretat



Missió seguretat

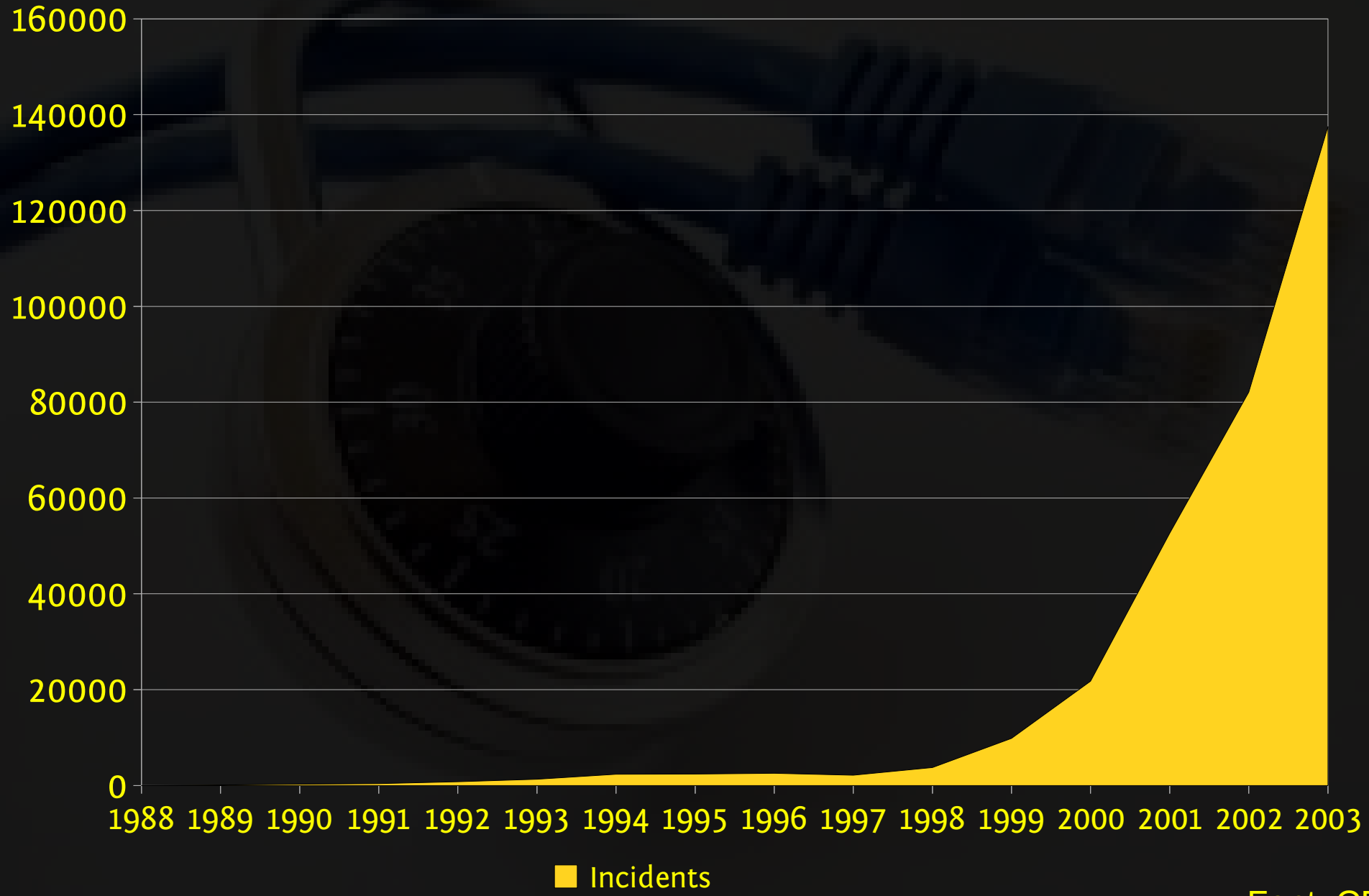
- Eliminar amenaces
- Detectar vulnerabilitats
- Abortar atacs
- Implantar salvaguardes
- Minimitzar risc

Gravetat



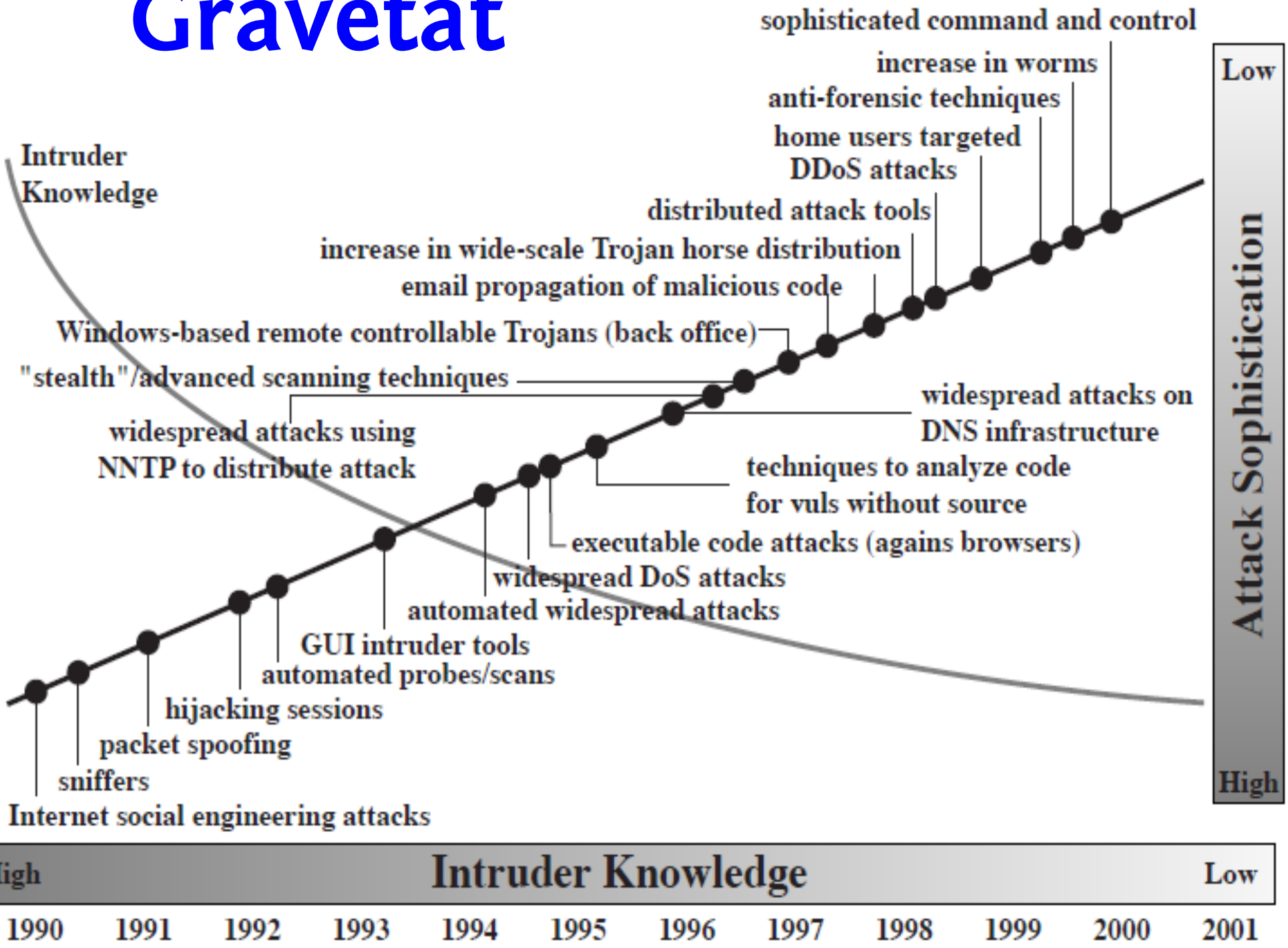
Font: CERT

Gravetat



Font: CERT

Gravetat



Source: CERT

Incidents de seguretat

- Intrusió als sistemes
- Violació d'autorització
- Implantació de trampes i cavalls de Troia
- Monitorització de les comunicacions
- Recollida d'informació
- Alteració de les comunicacions
- Interrupció del servei
- ...

Febleses

Físiques

Accés als dispositius: normalment els posa en MOLT perill.

Febleses

Hardware/Software

Errades en disseny, construcció i/o implementació poden deixar forats i problemes no controlats.

Febleses

Media

Podem perdre/ens poden robar: CDs/DVDs descontrolats, USBs usables, etc.

Podem llençar discs durs plens de dades als ordinadors de rebuig, etc.

Febleses

Transmissió/Emanació

Es factible interceptar dades radiades (WiFi/BT/etc.) o fins i tot, senyals elèctriques (Tempest, etc.)

MEGA Febleses

Humanes

Donar passwords per telefon, apuntar-los, deixar coses obertes, etc.

Enemics

Externs

- Hackers (pocs):
- Espionatge industrial/polític
- Terrorisme
- Criminals
- Virus/automàtics:
  - Spammers
  - botnets

Enemics

Interns

La major font de feblesa: empleats emprenyats.

Salvaguardes

- Avaluació del risc
- Disseny de polítiques de seguretat
- Implantació de mecanismes pasius i actius de protecció
- Implantació de mecanismes de monitorització i seguiment
- Resposta a incidents
- Recuperació d'incidents

Avaluació del risc

- Identificar i prioritzar d'actius
- Identificar vulnerabilitats
- Identificar amenaces i probabilitats
- Identificar contramesures
- Fer anàlisi cost/benefici

Avaluació del risc

- Què?
- Perquè?
- Valor?
- Amenaces?
- Riscs?
- Conseqüències?
- Escenaris d'atac/pèrdua?
- Cost de la pèrdua?

Tipus de política de seguretat

- Defensa per ocultació (Security by Obscurity)
- Defensa Perimetral (Perimeter Defense)
- Defensa en fondària (Defense in Depth)

Política de seguretat

- Procediments d'actuació general
- Procediments de control de seguretat
- Procediments de seguiment
- Procediments de resposta d'incidents

Mecanismes de protecció

- Serveis d'autenticació
- Serveis de control d'acces
- Serveis de confidencialitat
- Serveis d'integritat de dades
- Serveis de no repudi
- Serveis de protecció de servei

Mecanismes de protecció

- **Firewalls**: xarxa/detecció,bloqueig
- **Wrappers**: xarxa/host
- **Honeypots**: xarxa/detecció
- **Criptografia**: host,xarxa/confidencialitat
- **VPNs**: xarxa/confidencialitat
- **Eines forense**: host,xarxa/resposta
- **IDS**: host,xarxa/detecció,bloqueig
- **ACLs/Armoring**: host/detecció,bloqueig

...

Resposta a incidents

Ha de contemplar

Qui ha de respondre, com ho ha de fer, on s'ha de notificar.

Recuperació d'incidents

- Com recuperar dades, còpies, etc.
- Detectar quina informació està compromesa
- Valorar el cost de pèrdua