

{ Turvaliselt
arendamine }

Andri Möll



NutiKaitse



Turvavead



2. printsiip



NutiKaitse

Nõuded ja suunised arendamiseks
Avalikule ja erasektorile





**MAJANDUS- JA
KOMMUNIKATSIOONI-
MINISTEERIUM**



Vaata Maailma
Look@World Foundation



ENISA nutitelefonide turvalise arendamise juhis aluseks

Tõlkisime
Toimetasime
Lihtsustasime





nutikaitse.ee
nutikaitse.ee/suunised

67

Autentimine
Andmete kaitse seadmes
Andmete kaitse võrgus
Rakenduse kaitse

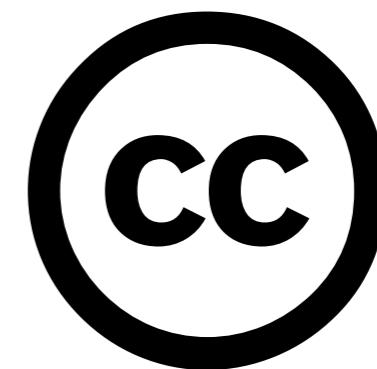




Tekstifailid

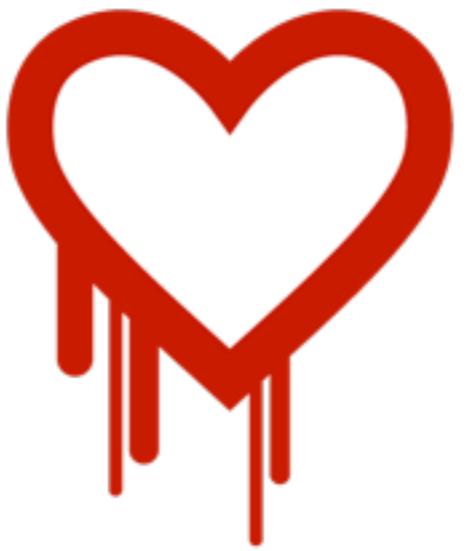


GitHub



Creative
Commons

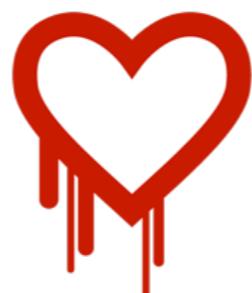




Turvavead

Turvavead

Strateegilised • Taktikalised
Universalsed • Äriloogikalised



Strateegiline või taktikaline viga

Vale asi õigesti või õige asi valesti
Viga disainis või viga implementatsioonis



Strateegiline või taktikaline viga

Formaalsus võimaldab automaatset analüüsia
Strateegiad tuleb manuaalselt analüüsida



Strateegiline või taktikaline viga

Taktikalisi vigu kergem ennetada
Programmeerimiskeele ja arhitektuuri roll ennetusel



Memory-managed keeltes ei esine
mälukasutusega seotud turvavigu

Puhvrite ületamine
Pointerite käsitluse vead



Tüübisteemid

Garantii, et ühe kasutaja andmed teisele ei tagastataks



Universalsed ja äriloogikalised vead

Igas ärivaldkonnas või ühes ärivaldkonnas



Universaalne viga

Injection rünnakud

Universaalsed andmelekked

Sisselogimisründed

...



Äriloogikaline viga

Tehingu kinnitamiseks kahe rolli nõue
Inventari koguste ligipääs valedele töötajale
Kargolaevade sihtpunktide konfidentsiaalsus

...



Universaalne viga

Rohkem uuritud

Kergem infot leida või analüüsni sisse osta

Küberturbeeksperdid kursis



Äriloogikaline viga

Ärisaladust või ärielist teab sinu firma või valdkond



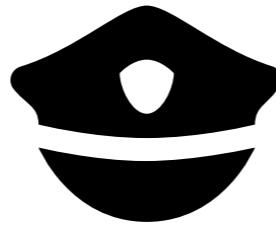
Testimistarkvara või tulemüürid ei kata strateegilisi vigu
Sisse toodud turvaekspert ei kata äriloogikat





Turvaline
ebaõnnestumine

Võrguliikluse krüpteerimine



SSL

Sertifikaadi väljastaja

Sertifikaadi nimi

Sertifikaadi kehtivus



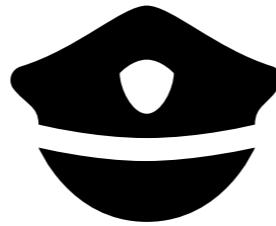
Online Certificate Status Protocol

Kontrollib sertifikaadi kehtivust väljastajalt
Kaitseb varastatud või kaotatud sertide eest



Online Certificate Status Protocol

Päringu ebaõnnestumise puhul ühendus õnnestub
Turvalisem on ebaõnnestumise puhul ühendus katkestada





```
OSStatus err;

if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
    goto fail;
    goto fail;

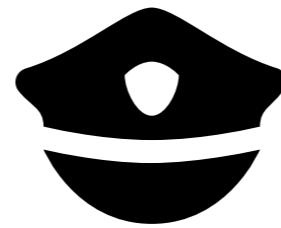
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
    goto fail;

fail:
    return err;
```

```
if (getPermission() == DENIED) { ... }  
else { ... }
```

```
if (getPermission() == ALLOWED) { ... }  
else { ... }
```

Piirang tuleb kiiremini välja kui luba



Protection of Information in Computer Systems (1975)

Jerome H. Saltzer, Michael D. Schroeder

The Protection of Information in Computer Systems

JEROME H. SALTZER, SENIOR MEMBER, IEEE, AND
MICHAEL D. SCHROEDER, MEMBER, IEEE

Invited Paper

Abstract - This tutorial paper explores the mechanics of protecting computer-stored information from unauthorized use or modification. It concentrates on those architectural structures—whether hardware or software—that are necessary to support information protection. The paper develops in three main sections. Section I describes desired functions, design principles, and examples of elementary protection and authentication mechanisms. Any reader familiar with computers should find the first section to be reasonably accessible. Section II requires some familiarity with descriptor-based computer architecture. It examines in depth the principles of modern protection.

Confinement
Allowing a borrowed program to have access to data, while ensuring that the program cannot release the information.

Descriptor
A protected value which is (or leads to) the physical address of some protected object.

Discretionary
(In contrast with nondiscretionary.) Controls on access to an object that may be changed by the creator of the object.

Domain



NutiKaitse

Vaata suunised üle
Anna tagasisidet



OWASP Mobile Security Project



AVOIDING THE TOP 10 SOFTWARE SECURITY DESIGN FLAWS

Iván Arce, Kathleen Clark-Fisher, Neil Daswani, Jim DelGrosso, Danny Dhillon,
Christoph Kern, Tadayoshi Kohno, Carl Landwehr, Gary McGraw, Brook Schoenfeld,
Margo Seltzer, Diomidis Spinellis, Izar Tarandach, and Jacob West



Building Security In Maturity Model



Security Engineering

Ross Anderson

SECOND EDITION

ج