Hacking

Erik Poll

Digital Security groep

Institute for Computing & Information Science

Radboud Universiteit Nijmegen

Wie is die gast?

Ik doe onderzoek naar & geef onderwijs over cybersecurity:

- **software security**

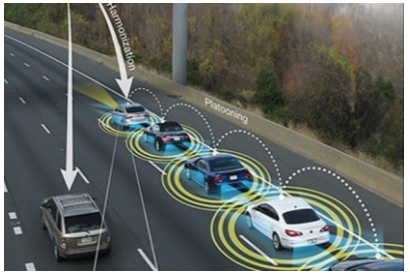
  ***Hoe* kunnen we software veiliger maken?**

  ***Waarom* is software zo onveilig?**

- **toegepast onderzoek**

  ***Hoe* veilig is een bepaald system? *Hoe* bepalen we dat?**

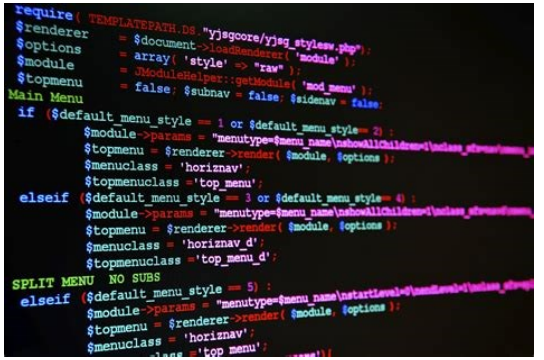
  ***Waarom* is het wel/niet veilig?**



Hoe hack je een computer system?

1. Val de gebruiker aan
   - bijv. phishing email
     om user-naam & wachtwoord te achterhalen
   - oftewel social engineering

2. Val de software aan
   - zoek zwakheid & exploiteer deze
   - het 'echte' hacking



Wat is hacken?

Hacken = iets gebruiken op een manier of voor een doel wat *niet* de bedoeling was

Voorbeelden van hacking

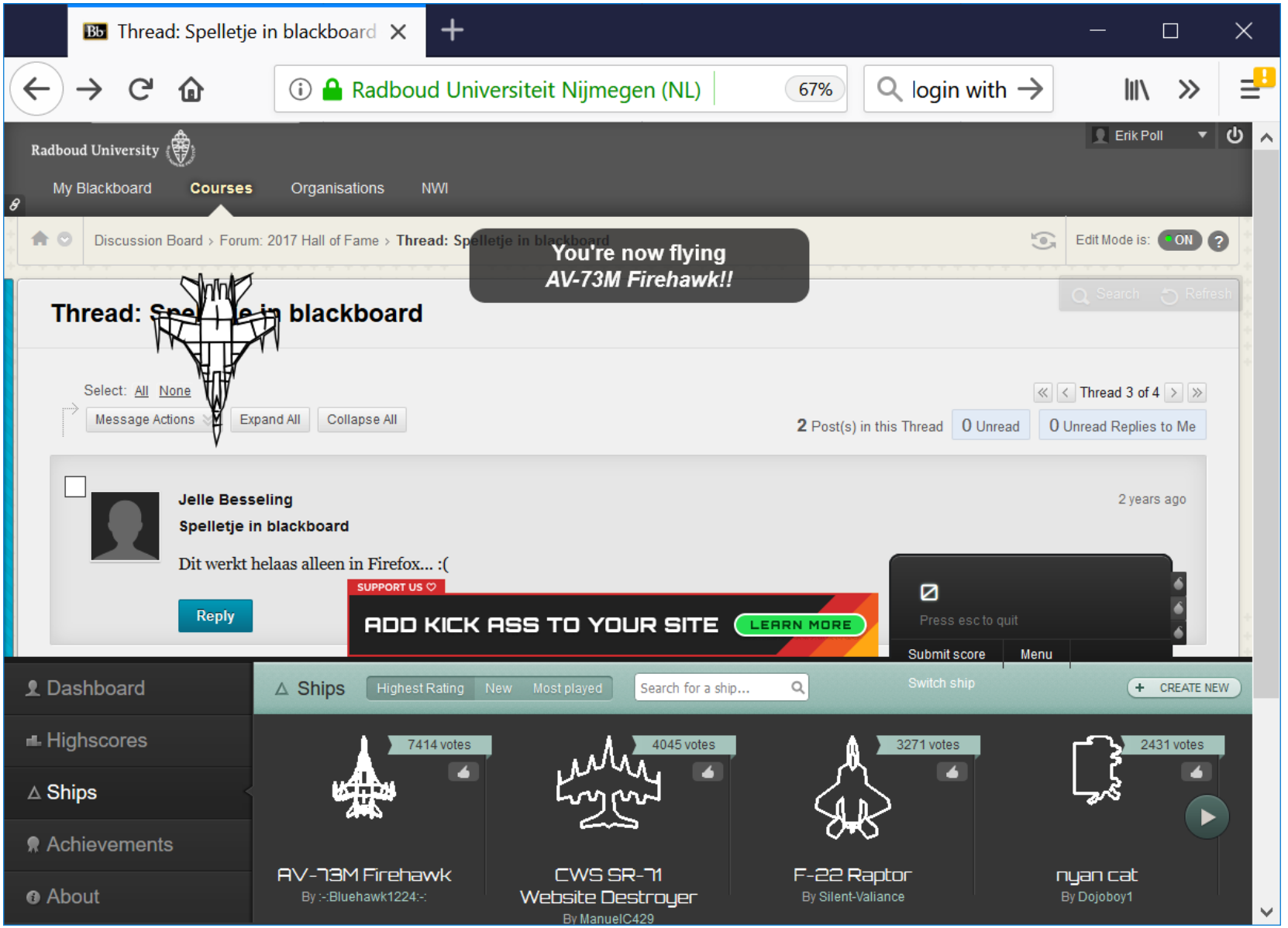
[Simone Giertz, shitty robot]

suikerspin maken met harde schijf
https://www.youtube.com/watch?v=D3sTjj1eeAA

Oplaadpaal ge/misbruiken om wafels te bakken

[Matthias Dalheimer, CCC'2018, https://evsim.gonium.net]

Hacking: game in Radboud onderwijswebsite



Hacken & software

Software maakt computers essentieel anders dan andere apparaten

Bijv:

- Gehackte site kun je HERPROGRAMMEREN om VAN ALLES te doen
  - gamen, je cijfers veranderen, bitcoin minen, gebruiken als platform om ander systemen te hacken of DoSen, …
- Gehackte boormachine, afwasmachine, harde schijf, … kan alleen maar beperkte variaties van hetzelfde doen
  - tenzij er een computer & software in zit …

Voorbeeld hack uit onze groep (1)

deVerdieping
Trouw
zaterdag 12 april 2008
66ste jaargang nr 19451
www.trouw.nl

• Achterhalen van gegevens van veel kaarten in korte tijd blijkt wel degelijk mogelijk

Kraken ov-chip secondenwerk

Alle gegevens van een ov-chip blijken nu met een druk op de knop te achterhalen. Het vertrouwen in de kaart loopt een nieuwe deuk op.

Vincent Dekker

Nieuwe ontdekkingen aan de Nijmeegse Radboud Universiteit hebben van het kopiëren van de ov-chipkaart een secondenklus gemaakt. Grootschalig misbruik is hiermee nu mogelijk.

Begin maart werd bekend dat de Nijmeegse onderzoekers toegangspassen konden kopiëren door een kwartier bij een leesapparaat speciale metingen te doen.

De nieuwe methode werkt veel sneller, het afluisteren van één enkele transactie levert voldoende informatie om alle geheime sleutels binnen seconden mee uit te rekenen.

De gegevens op een ov-chipkaart zijn op twee manieren beveiligd. De eerste horde is de geheime versleutelmethode van de kaart. Die beveiliging was begin maart al gebroken. Andere gegevens, zoals details over gemaakte reizen en het saldo op de kaart, staan in aparte 'sectoren' die met afzonderlijke sleutels zijn beveiligd.

Ook deze tweede beveiliging is nu gebroken. De onderzoekers in Nijmegen hebben bovendien een methode gevonden om dat niet meer in een kwartier op een krachtige computer maar in luttele seconden op een laptop te kunnen doen.

Wouter Teepe is als wetenschappelijk medewerker het gezicht van het onderzoek naar de ov-chipkaart. Teepe heeft zijn informatie doorgegeven aan de collega's van de universiteit van Londen die de afgelopen weken een zogeheten contra-expertise hebben uitgevoerd op een TNO-

Nijmeegse onderzoekers kunnen nu in luttele seconden details over bijvoorbeeld het saldo van een ov-chip achterhalen. FOTO ROBIN VERHEIJEN

verkeer en waterstaat om onze kennis met de mensen in Londen te delen", aldus Teepe. „Op 28 maart hebben we een demonstratie gegeven om te laten zien dat we het echt konden."

Toen hadden Teepe en zijn groep voor het decoderen van een enkele sleutel nog een minuut nodig. „Inmiddels achterhalen we een enkele sleutel. Het wordt nu mogelijk om ov-chipkaarten op grote schaal te 'skimmen', zoals ook wel bij bankpasjes gebeurt. Vlak bij een ov-chiplezer kan in het geniep een tweede lezer worden geplaatst die alle informatie op de aangeboden ov-chipkaarten opvangt, decodeert en opslaat.

Zo zou je met dure duizenden euro's

kopie van een andere kaart gebruiken, waar de kans op ontdekken wel heel erg klein maakt."

TLS, het bedrijf dat de ov-chipkaart in Nederland introduceert, kan in eigen computers elke nacht het gebruik van de individuele kaarten volgen. Worden er gekke dingen geïnitieerd, dan kan TLS de betrokken

dende eigenaar plotseling de trein of tram niet meer in komt. Als dat vaak gebeurt, zal de acceptatie van de ov-chipkaart snel afnemen.

De onderzoekers in Londen zijn inmiddels klaar met hun contra-expertise. De komende week zal hun rapport aan de Tweede Kamer worden aangeboden. Volgens ingewijden hebben Kamerleden grote druk de

Nieuwe afstudeeropdracht:

Afstudeerscripties van Roel Verdult & Gerhard de Konig Gans

Voorbeeld hack uit onze groep (2)

Kunnen we de ABN.AMRO e-dentifier met USB kabel gebruiken als gewone smartcard-lezer?

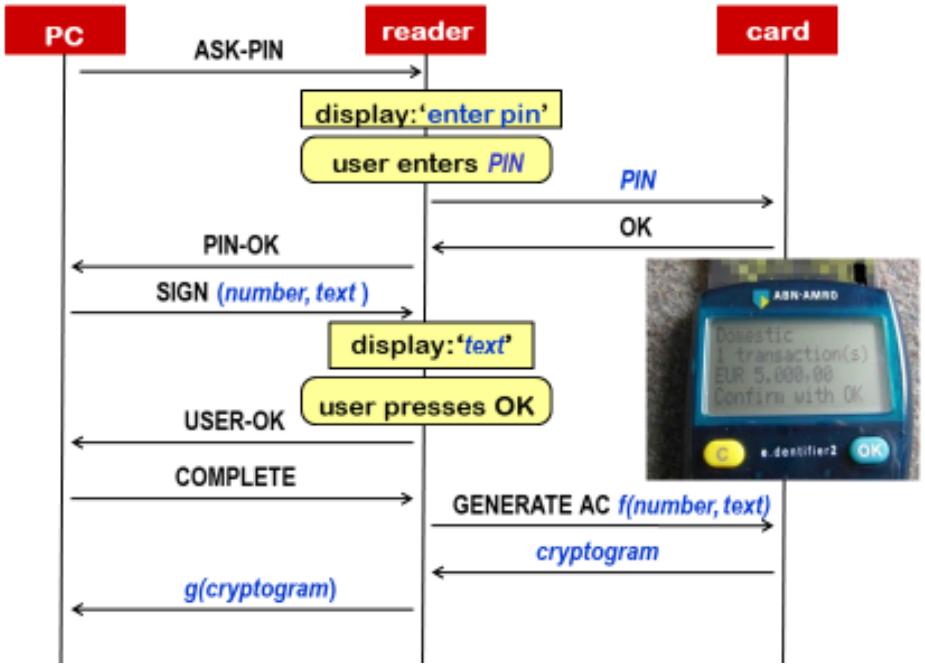
Afstudeerscriptie Arjan Blom

Hoe werkt dat ding? aka reverse-engineering

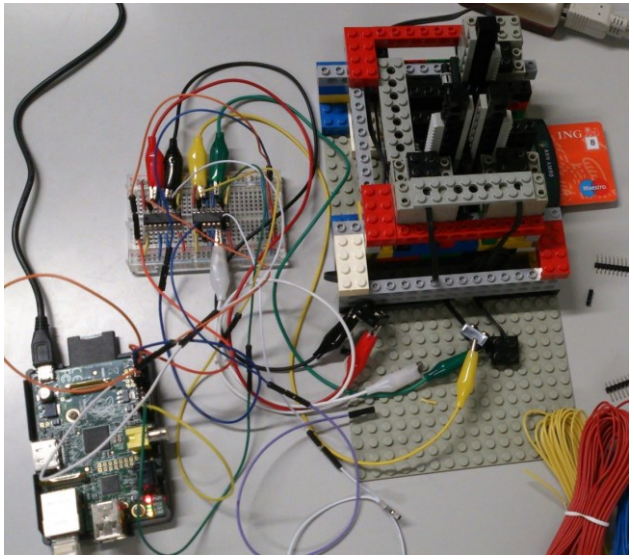
Berichten onbeveiligd over USB kabel en zijn dus aan te passen

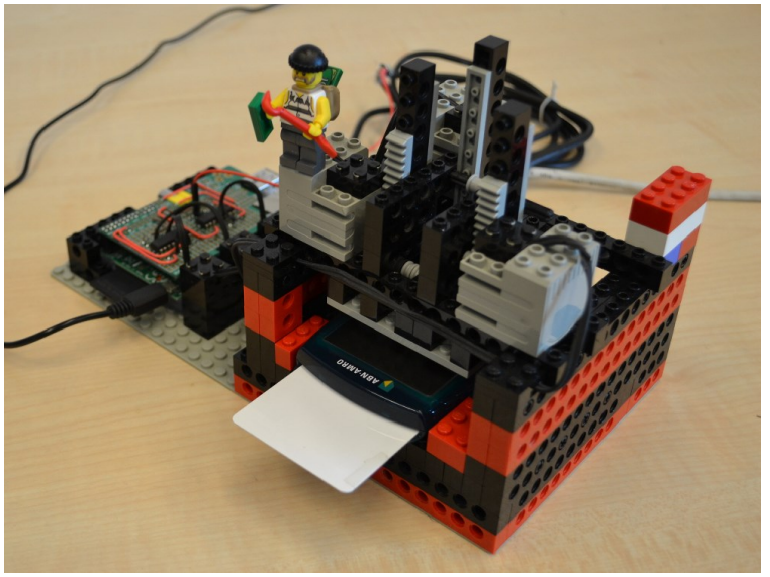
Oeps…

Malware op de computer kan via USB kabel op de OK knop drukken!



Kunnen we deze fout automatisch ontdekken?

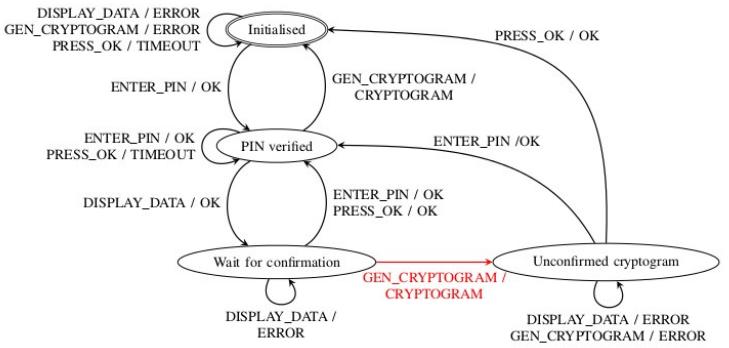




Project van exchange studenten Georg Chalupar & Stefan Peherstorfer

https://tinyurl.com/legolearning

[Automated Reverse Engineering using LEGO, WOOT 2014]



Misdrijven & responsible disclosure

NB hacken van computer van iemand anders is een misdrijf

Voortvluchtige veroordeelde cybercrimineel aangehouden in Nederland

Gepubliceerd op:
11-06-2021 | 10:47

Breda, Amsterdam - De in 2019 voor cybercriminaliteit veroordeelde J.V. is op woensdag 9 juni aangehouden in Amsterdam. In 2019 werd de 30-jarige vrouw een gevangenisstraf opgelegd van vijf jaar. Ze was voortvluchtig sinds haar veroordeling. De politie is nog op zoek naar de mannelijke medeverdachte, de 26-jarige Amsterdammer I.T.

Vier jaar cel en 50.000 euro boete geëist tegen bouwer phishingsites

Nieuws *04-06-2021*

DIVD

Dutch Institute for Vulnerability Disclosure

Meer te weten komen?

Zelf hacken?

- picoctf.org
- overthewire.org Bandit
- hackthebox.eu
- …

En daarna meedoen aan

CTFs (Capture-the-Flags)

- ctftime.org
- …

Podcast tip: